JONATHAN K. LEVINE (SBN 220289)
jkl@pritzkerlevine.com
ELIZABETH C. PRITZKER (SBN 146267)
ecp@pritzkerlevine.com
SHIHO YAMAMOTO (SBN 264741)
sy@pritzkerlevine.com
PRITZKER LEVINE LLP
180 Grand Avenue, Suite 1390
Oakland, CA 94612
Telephone: (415) 692-0772
Facsimile: (415) 366-6110

DANIEL C. GIRARD (SBN 114826)
dcg@girardgibbs.com
AMANDA M. STEINER (SBN 190047)
as@girardgibbs.com
ELIZABETH A. KRAMER (SBN 293029)
eak@girardgibbs.com
ANDRE M. MURA (SBN 298541)
amm@classlawgroup.com
GIRARD GIBBS LLP
601 California Street, Suite 1400
San Francisco, CA 94104
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

STEVEN N. WILLIAMS (SBN 175489)
swilliams@cpmlegal.com
MATTHEW K. EDLING (SBN 250940)
medling@cpmlegal.com
ALEXANDRA P. SUMMER (SBN 266485)
asummer@cpmlegal.com
COTCHETT, PITRE & McCARTHY, LLP
San Francisco Airport Office Center
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Telephone: (650) 697-6000
Facsimile: (650) 697-0577

Plaintiffs' Interim Co-Lead Counsel

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NORTHERN CALIFORNIA

SAN JOSE DIVISION

IN RE: LENOVO ADWARE LITIGATION

This Document Relates to All Cases

Case No. 5:15-md-02624-RMW

CLASS ACTION

CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

Plaintiffs, by and through their undersigned attorneys, hereby complain against Defendants Lenovo (United States) Inc. and Superfish Inc., on behalf of themselves and all others similarly situated, as follows. Plaintiffs' allegations are based upon information and belief, except as to their own actions, which are based on knowledge. Plaintiffs' information and belief is based on the investigation of their undersigned counsel, the documents produced in discovery to date, and facts that are a matter of public record.

NATURE OF THE CASE

1. This is a nationwide consumer class action against Lenovo, the largest computer manufacturer in the world, and Superfish, a privately-held Silicon Valley company that develops, sells, and operates computer adware programs. Earlier this year, consumers and computer experts discovered that Lenovo had sold more than 800,000 computers in the United States that included, without the consumers' knowledge or consent, a software program that computer security experts consider to be spyware or malware.

2. The program was Superfish's VisualDiscovery software. It functioned by intercepting data sent between a computer user and a website, redirecting it for analysis to generate relevant advertisements, and then transmitting those advertisements back to the user's computer where they would be injected into the web browser. Lenovo agreed to install VisualDiscovery on its consumer notebook computers in exchange for [redacted]

3. Lenovo did not disclose to consumers that it was installing VisualDiscovery on its computers (although other third-party software was listed on Lenovo's website), and VisualDiscovery was buried deep within the operating system to avoid detection by anti-malware programs.

4. Lenovo knew, before it sold any computers with VisualDiscovery installed, that the program interfered with users' secure connections to the internet, that it relied on code written by a much-criticized software company that touted its ability to hijack user data that consumers and computer experts disapproved of VisualDiscovery's underlying technology, that Superfish had a poor reputation, and that the program was very difficult for users to remove. None of these facts deterred Lenovo, which

undertook significant efforts to ensure that the program was not discovered instead of deciding not to install it in the first place.

5. VisualDiscovery had a materially negative impact on the Lenovo computer models on which it was installed. From a performance perspective, the program increased CPU usage, which increased power consumption. Because all of the computers on which it was installed were laptop computers that relied on a battery, the increased CPU usage decreased both the amount of time an affected computer could operate between charges and the lifespan of the battery. In addition, VisualDiscovery [redacted], caused certain web pages to load incorrectly and in many instances, blocked web pages entirely. When users were able to connect, they were subjected to unwanted advertising and pop-ups that were difficult to remove and to stop.

6. From a security and privacy perspective, VisualDiscovery was a disaster. In order to operate as intended, the program, without the user's knowledge or consent, broke the secure connection a user thought he or she was creating with an established website, rerouted that connection through a Superfish server and then sent results back to the user in a way that hid the fact that the search had been monitored, hijacked and altered. The process by which Superfish did all this relied on a single common digital key and weak password that were shared by all of the computers and easily accessible to a computer hacker, who could use them to access an affected computer on any public network and collect whatever information was being transmitted at the time.

7. Earlier this year, the truth about the program and Lenovo's relationship with Superfish finally emerged. Lenovo has since apologized, admitted that what it had done was wrong, admitted that it had failed to conduct due diligence on VisualDiscovery before it was installed, and admitted that the program created high security risks for the 800,000 computers on which it was installed.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this matter pursuant to 18 U.S.C. § 1030(g) and 28 U.S.C. § 1331.

9. Venue is proper in this District under 28 U.S.C. § 1391(b) and (c). A substantial portion of the events and conduct giving rise to the violations of law occurred in this District, defendant

Superfish is headquartered in this District, and Lenovo conducts business in and sold affected Lenovo notebook computers directly to consumers in this District. Additionally, venue is appropriate pursuant to 28 U.S.C. § 1407 and the Order of the United States Judicial Panel on Multidistrict Litigation. (Dkt. No. 108).

PARTIES

I. Plaintiffs

10. Plaintiffs are consumers who purchased one or more Lenovo computers in late 2014 or early 2015 on which VisualDiscovery was installed.

11. Plaintiff Richard Krause, a resident of Illinois, purchased from Lenovo.com a Lenovo notebook computer on which VisualDiscovery was installed and has been damaged thereby.

12. Plaintiff John Whittle, a resident of Arizona, purchased through Ebay.com a Lenovo notebook computer on which VisualDiscovery was preinstalled and has been damaged thereby.

13. Plaintiff Rhonda Estrella, a resident of California, purchased from a Best Buy in California a Lenovo notebook computer on which VisualDiscovery was installed and has been damaged thereby.

14. Plaintiff Jessica Bennett, a resident of California, purchased from a Best Buy in California a Lenovo notebook computer on which VisualDiscovery was installed and has been damaged thereby.

15. Plaintiff Robert Ravencamp, a resident of Missouri, purchased from Lenovo.com a Lenovo notebook computer on which VisualDiscovery was installed and has been damaged thereby.

16. Plaintiff Vincent Wong, a resident of New York, purchased from Lenovo.com a Lenovo notebook computer on which VisualDiscovery was installed and has been damaged thereby.

17. "Plaintiffs" refers collectively to the named plaintiffs identified in paragraphs 11 through16 above.

II. Defendants

18. Defendant Lenovo (United States) Inc. is a Delaware corporation with its principal place of business in Morrisville, North Carolina. Lenovo is a wholly-owned subsidiary of Lenovo Holding Company, Inc., which is a subsidiary of Lenovo Group Limited, a Hong Kong corporation with its

principal place of business in Beijing, China. Lenovo Group is a principal subsidiary of Legend Holdings Limited, a Beijing-based conglomerate whose largest shareholder is the Chinese government.

19. Defendant Superfish Inc. is a Delaware corporation with its principal place of business in Palo Alto, California.

FACTUAL ALLEGATIONS

I. Background on Lenovo

20. Lenovo was founded in 1984 in Beijing, China, by the Chinese Academy of Sciences, an agency of the government of the People's Republic of China. Operating under its original name - Legend Holdings – Lenovo's original business was to import computer products. In 1990, Legend Holdings began to manufacture its own computer products. By 1996, it was the largest personal computer manufacturer in mainland China.

21. Legend Holdings went public on the Hong Kong Stock Exchange in 1994, but remained majority controlled by the Chinese Academy of Sciences after its initial public offering. In 2003, Legend Holdings changed its name to Lenovo.

22. In 2005, Lenovo purchased IBM's personal computing division, including IBM's ThinkPad line of laptops, making Lenovo the third-largest computer maker in the world. By 2013, Lenovo was the largest PC manufacturer in the world and it remains the largest today.

23. Legend Holdings, now a multinational conglomerate based in Beijing, China, remains Lenovo's largest shareholder, owning more than one-third of the company. Legend Holdings refers to Lenovo in its securities filings as a "Principal Subsidiary." Legend Holding's largest shareholder remains the Chinese government.

24. Lenovo's market dominance has come at a steep price for the company and the millions of consumers that have purchased Lenovo computers. Lenovo has recently been slashing prices on its computers in a competitive "race to the bottom."[1] Some of the Lenovo computers at issue in this litigation retail for just $349.95, a price point well below the "historically low levels" of $410–$430 per

[1] Brad Chacos, *Bloatware: Why Computer Makers Fill Your PC With Junk, and How to Get Rid of It*, Feb. 26, 2015, PC World, http://www.pcworld.com/article/2889292/ bloatware-why-computer-makers-fill-your-pc-with-junk-and-how-to-get-rid-of-it.html (last visited Aug. 26, 2015).

computer reported just a year ago. Computer vendors like Lenovo make "little to no money on such slim margins."[2]

25. In an effort to offset its discounted prices, Lenovo now routinely accepts payments from software developers like Superfish to preload its computers with the developers' programs. Commonly referred to as "bloatware" or "crapware," this preloaded software often loads at startup, wastes memory, creates potential conflicts with other applications, and slows the performance of computers on which it is installed.

26. Despite these negative effects on performance, Lenovo continues to preload such software onto its computers because, as Forbes reported, "there's a lot of money to be earned by simply bundling extra 'crapware' onto people's PCs."[3]

27. Lenovo's installation of VisualDiscovery is not the first, last or only time that Lenovo has surreptitiously installed software and hardware on Lenovo computers that (i) allows Lenovo and others unauthorized access those computers after sale, and (ii) creates potential security vulnerabilities in those computers.

28. In 2006, the U.S. Department of State purchased 16,000 Lenovo computers, but then declared those computers too compromised for secure information and communications channels. The National Security Agency in particular was concerned about state-sponsored malicious circuitry in the computer hardware. The U.S. government determined that the Lenovo computers it had purchased contained these circuits, as well as tiny antennas and firmware that allowed back-door access to the computers—and to any network connected to the computers.

29. Lenovo computers are banned for use in the intelligence and defense services of the United States, Australia, Canada, New Zealand and the United Kingdom. According to the Australian Financial Review, "the ban was introduced in the mid-2000s after intensive laboratory testing of its equipment allegedly documented 'back-door' hardware and 'firmware' vulnerabilities in Lenovo

---

[2] *Id.*

[3] Thomas Fox-Brewster, *Superfish: A History of Malware Complaints and International Surveillance*, Feb. 19, 2015, Forbes, http://www.forbes.com/sites/thomasbrewster/ 2015/02/19/superfish-history-of-malware-and-surveillance/ (last visited Aug. 26, 2015).

chips."[4] IT security industry analyst James Turner told the Australian Financial Review in that same article that "the fact that Lenovo kit is barred from classified networks is significant, and something the private sector should look at closely."[5]

30. And, between October 2014 and April 2015, Lenovo sold 23 different Lenovo computer models to consumers in the United States that included a previously undisclosed program called Lenovo Service Engine ("LSE"). LSE was built directly into the firmware of the Lenovo computers, at the lowest level of the operating system called the BIOS, which is invisible even to Windows. BIOS is what launches when a computer is turned on, before Windows loads, and its purpose is to ensure that the computer was shut down properly previously, that the hard drive is not corrupted, and that it is safe to launch Windows and all of the other programs loaded on the computer.

31. LSE allowed Lenovo, without the consumer's knowledge or consent, to automatically connect the Lenovo computer to the internet to download and install drivers, a system optimizer and any other software Lenovo wanted or had deals with third-party developers to put on the computer.[6] As one Lenovo computer user complained "I had this happen to me a few weeks ago, on a new Lenovo laptop, doing a clean install with a new SSD, Windows 8 DVD and Wi-Fi turned off. I couldn't understand how a Lenovo service was installed and running. Delete the file and it reappears on reboot. I've never seen anything like this before. Something to think about before buying Lenovo."[7]

32. LSE also allowed Lenovo to determine the details of what was running on each consumer's Lenovo computer. "The software installed by Lenovo Service Engine didn't just include updates to drivers, firmware, and pre-installed apps, but also sent 'system data to a Lenovo server to help [Lenovo] understand how customers use [its] products.' While Lenovo says it's not collecting

---

[4] Christopher Joye et al., *Spy Agencies Ban Lenovo PCs on Security Concerns*, Jul. 29, 2013, Australian Financial Review, http://frg.admin.afr.com/p/technology/spy_agencies_ban_lenovo_pcs_on_security_HVgcKTHp4bIA4ulCPqC7SL (last visited Aug. 28, 2015).

[5] *Id.*

[6] Alex Hern, *Lenovo Does It Again as LSE Component Removed After Security Fears*, Aug. 14, 2015, The Guardian, http://www.theguardian.com/technology/2015/aug/14/lenovo-service-engine-pre-installed-security-superfish (last visited Sept. 28, 2015).

[7] Chris Williams, *CAUGHT: Lenovo Crams Unremovable Crapware into Windows Laptops – By Hiding it in the BIOS*, Aug. 12, 2015, The Register, http://www.theregister.co.uk/2015/08/12/lenovo_firmware_nasty/ (last visited Sept. 28, 2015).

personally identifiable information, the collection itself may be something customers aren't aware of, and until now haven't had any control over."[8]

33. While Lenovo has attempted to downplay this latest violation of its customers' trust and privacy, industry experts have been more forthcoming, with articles titled: *Lenovo's Service Engine marks yet another bloatware blunder for the company*; *Lenovo does it again as LSE component removed after security fears*; *Caught: Lenovo crams unremovable crapware into Windows laptops – by hiding it in the BIOS*; and *Lenovo used Windows anti-theft feature to install persistent crapware.*[9]

II. Background on Superfish and VisualDiscovery

A. Superfish

34. Superfish is a privately held software development company with offices in Palo Alto, California, and Petah Tikva, Israel.[10] The company "develops image-to-image search technology that enables consumers to search for items based on the appearance of the item, rather than a text based description."[11] In 2013, Superfish's revenue reached $35.3 million—an increase of 26,000 percent over the previous three years.[12] Superfish was ranked 64th on Forbes's list of the most promising American companies of 2015, reporting 2014 revenues of $38 million. According to Forbes, "[i]t pays to be invasive these days."[13]

35. Superfish was co-founded by Adi Pinhas and Michael Chertok—two "veterans of the video surveillance industry" with a history of questionable privacy practices.[14] In 1999, they founded

---

[8] Jared Newman, *Lenovo's Service Engine Makes Yet Another Bloatware Blunder for the* Company, Aug. 12, 2015, PC World, http://www.pcworld.com/article/2969365/security/lenovos-service-engine-marks-yet-another-bloatware-blunder-for-the-company.html (last visited Sept. 28, 2015).

[9] Newman, *supra*; Hern, *supra*; Williams, *supra*; Peter Bright, *Lenovo Used Windows Anti-theft Feature to Install Persistent Crapware*, Aug. 12, 2015, Ars Technica, http://arstechnica.com/information-technology/2015/08/lenovo-used-windows-anti-theft-feature-to-install-persistent-crapware/ (last visited Sept. 28, 2015).

[10] After the facts giving rise to this litigation became public, Superfish changed its name to JustVisual. For the purposes of this complaint, Superfish refers also to its successor, JustVisual.

[11] Defendant Superfish, Inc.'s Response to Motion for Transfer of Actions, MDL No. 2624, Dkt. No. 45 at p. 2.

[12] Nicole Perlroth, *How Superfish's Security-Compromising Adware Came to Inhabit Lenovo's PCs*, Mar. 2, 2015, NY Times, http://nyti.ms/1wGVbty (last visited Aug. 26, 2015).

[13] Fox-Brewster, *supra*.

[14] *Id.*

Vigilant Technology, which "invented digital video recording for the surveillance market" and reports contracts with the United States military, casinos, prisons and several Israeli government organizations, among others.[15] Before founding Vigilant, Pinhas worked at Verint, an intelligence company. While there, he carried out "signal processing research" in which he would analyze information disseminated through telephone lines.[16]

36. In 2006, Pinhas and Chertok founded Link-It—a start-up designed to be a "visual search" engine for images "[m]uch in the same way that Google is a search engine for text, Siri for voice, and music discovery apps like Shazam help people match songs they hear on the radio to an artist and song title . . . ."[17] In 2009, Pinhas and Chertok renamed Link-It as Superfish.

37. VisualDiscovery is not the first Superfish program to inspire a backlash by consumers and industry experts. A predecessor program called WindowShopper was widely criticized as unwanted malware that "bombarded users with annoying ads and diverted them to websites they didn't want to visit."[18]

38. According to David Auerbach, a technology writer and software engineer, Superfish "has a long history of disseminating adware, spyware, malware, and crapware."[19] Computer security researcher Robert Graham, who was able to obtain and break the security of the VisualDiscovery root certificate in only a few minutes, is even more critical of the company:

> The company claims it's providing a useful service, helping users do price comparisons. This is false. It's really adware. They don't even offer the software for download from their own website. It's hard Googling for the software if you want a copy because your search results will be filled with help on removing it. The majority of companies that track adware label this as adware.[20]

---

[15] Fox-Brewster, *supra*.
[16] Fox-Brewster, *supra*.
[17] Perlroth, *Superfish's Security-Compromising Adware*, *supra*.
[18] CBS/AP, *Microsoft, Lenovo Scramble to Protect Users from Superfish Security Flaw*, Feb. 22, 2015, http://www.cbsnews.com/news/microsoft-lenovo-superfish-security-flaw/ (last visited Aug. 26, 2015).
[19] David Auerbach, *You Had One Job, Lenovo*, Feb. 20, 2015, Slate, http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_why_it_s_one_of_the_worst_consumer_computing_screw.html (last visited Sept. 29, 2015).
[20] Jennifer LeClaire, *Lenovo PCs Ship with Nasty Malware, Putting User Data at Risk*, Feb. 19, 2015, Sci-Tech Today, http://www.sci-tech-today.com/story.xhtml?story_id=11000CA8NKRU (last visited Sept. 29, 2015).

B. The VisualDiscovery Program

39. Superfish claims that VisualDiscovery was loaded onto Lenovo computers in order to "enhance the user experience." But the program was not available to consumers directly and there was no natural consumer demand for the program.

40. VisualDiscovery intercepts and scans a user's web traffic to inject unauthorized advertisements into the user's web browser. The program runs constantly on the Lenovo computer to detect web traffic and loads specially-designed JavaScript into the browser to access and control the data being transmitted over the internet.

41. The VisualDiscovery JavaScript runs throughout and has full access to every webpage the user visits, including any form content entered, usernames and other details such as cookies. This JavaScript allowed VisualDiscovery to examine the content of a webpage the user was on, and send information to Superfish's servers.

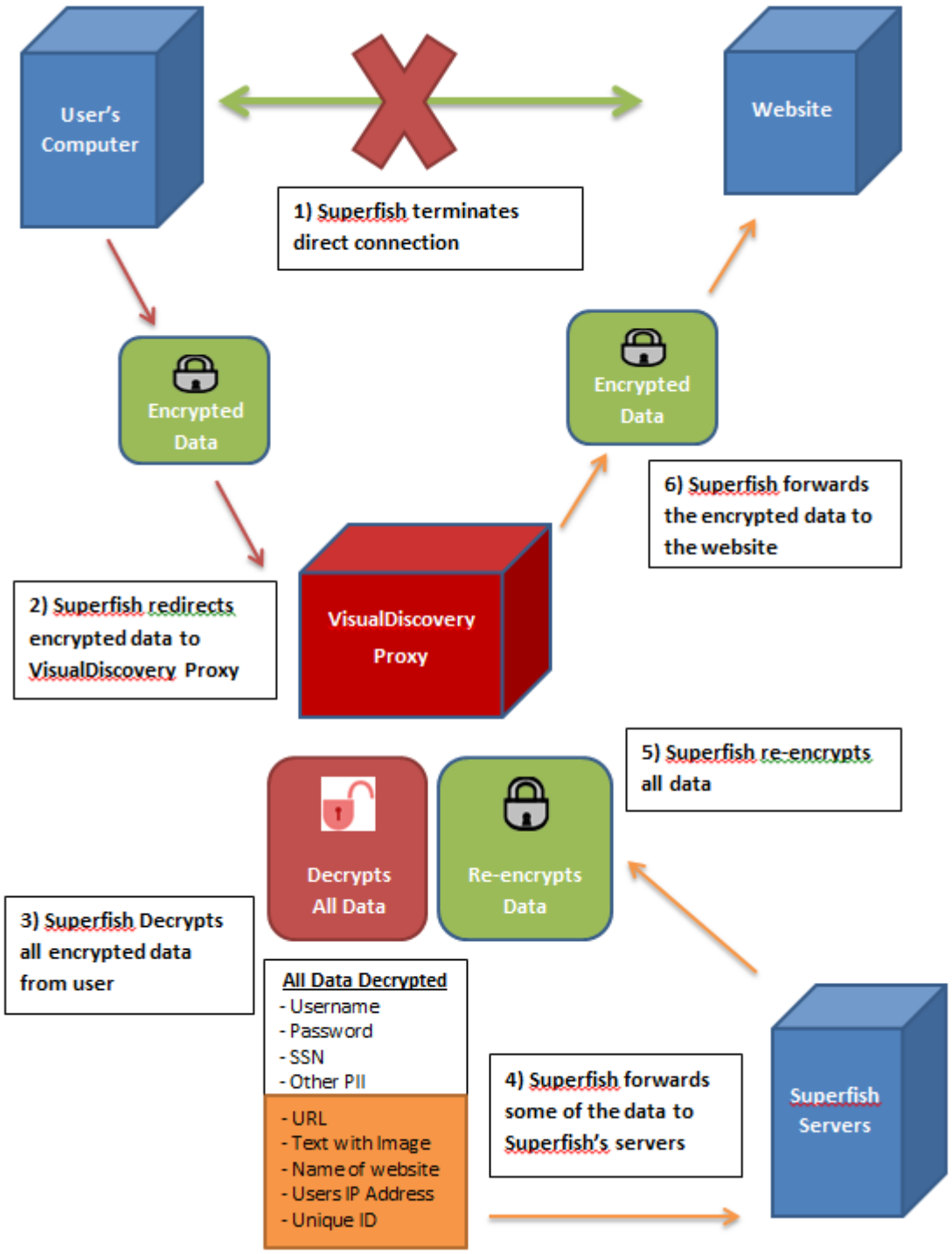
42. The information was then analyzed to generate purportedly relevant advertisements that were sent back to the user and injected either as part of the webpage or in a pop-up ad; for example:

43. Superfish was allegedly committed to only injecting the VisualDiscovery JavaScript on online shopping sites. But once the VisualDiscovery JavaScript inserted into a webpage, it was authorized to do virtually anything to a user's browser and did not distinguish between shopping websites and other websites.

44. VisualDiscovery's technology utilized a "proxy" component to be the hidden intermediary between the user and the intended server, intercepting and redirecting network traffic.

45. The VisualDiscovery proxy thus handled each transmission to and from a user's browser, whether encrypted or unencrypted. Unlike other proxies, however, in which encrypted webpage traffic remains encrypted and passes through without decryption from the originating server to the user's browser, the VisualDiscovery proxy acted like what is known as a Man-in-the-Middle ("MitM") proxy.

46. Specifically, when a user sought an encrypted connection to a website from his or her browser, the connection was handled directly by VisualDiscovery. Where there should have been one encrypted connection between the user's browser and the website, VisualDiscovery would create two: one between the browser and the VisualDiscovery proxy, and another between the proxy and the website. Encrypted information sent from the user's browser would be decrypted and read by the VisualDiscovery proxy. The proxy re-encrypted and forwarded the information to the website. Similarly, VisualDiscovery would decrypt and read information sent by the website, then re-encrypt and forward the information to the user's browser. VisualDiscovery would thus trick both the browser and the website into thinking it had a direct encrypted connection with the other. The diagram below illustrates how VisualDiscovery altered the flow of information between the user's browser and the web address server:



47. Secure information from an encrypted HTTPS connection cannot be decrypted without the authority to do so and the decryption code. In order to allow its proxy to decipher an otherwise encrypted connection, VisualDiscovery also had to install a root-certificate authority in order to give Superfish the appearance that it had the authority to decrypt enciphered information.

48. HTTPS is the protocol for securing communications over the internet. The main purpose for HTTPS is to authenticate a visited website and to protect the privacy and integrity of exchanged data. HTTPS provides a reasonable guarantee that one is communicating with precisely the website that one intends to communicate with as well as ensuring that the contents of the communications between the user and website cannot be read or forged by a third party.

49. HTTPS consists of communications over HTTP within a connection encrypted by the Secure Sockets Layer protocol, or its successor the Transport Layer Security protocol (collectively, "SSL"). Information on a HTTPS page is encrypted into scrambled or enciphered information by mathematical formulas called cryptographic algorithms, or ciphers and numbers called "keys". This information cannot be comprehended without having the appropriate key to unscramble and decipher the algorithms.

50. When a user logs onto a HTTPS website, the user receives what is called a public key, along with all the data that the browser displays. The public key allows a user to encrypt information for transmission or to verify a digital signature. There is a matching private key, held by the website owner, allowing the website utilizing the encryption to decrypt the information as well as to create a digital signature. These keys are used in the SSL protocol to activate a secure session between a browser and the web server.

51. In order to verify that the public key from a HTTPS website is actually from the web page the user is searching for, the public key is stored on a digital certificate. A digital certificate is a file that contains the identity credentials to help websites, people, and devices represent their authentic online identity. A digital certificate is used to authenticate the ownership of a HTTPS-encrypted page, essentially associating domain names (the identities) with a particular public key. Digital certificates prevent another from presenting their own public key and pretending to be the server a user is trying to reach. Digital certificates are signed, or vouched for, by a certificate authority.

52. A certificate authority is an entity that issues and manages security credentials and digital certificates as a third party, trusted both by the owner of a digital certificate and by the party relying upon the certificate. A certificate authority's obligation is to verify a website owner's credentials, so that users and relying parties can trust the information in the certificate authority's digital certificates

prior to establishing a secured connection. The five largest certificate authority providers are Comodo, Symantec, GoDaddy, GlobalSign, and DigiCert.[21]

53. Any browser or software that uses HTTPS needs a way to verify the digital certificates that link domain names to the public keys they use. This is accomplished by having a list of "root" certificate authorities preinstalled and maintained by the operating system that can sign digital certificates that the browser will trust. These root certificate authorities, as determined by the browser's publisher, are the authoritative entities from which a web browser knows how to trust a HTTPS website.

54. Thus, when a user opens a HTTPS webpage, the user receives the public key and all the data the browser receives from the HTTPS webpage, as well as the certificate authority's digital signature of the public key. Because the browser will have in its possession the public key of the certificate authority and can consequently verify the certificate authority's signature, the user can also assume that the particular public key does indeed belong to whoever is identified in the digital certificate.

55. VisualDiscovery could not inject its JavaScript into an HTTPS-secured webpage without first being able to decipher and read the encrypted information. Superfish lacked the technical expertise to get around this obstacle, and so enlisted the help of another company, B. W. Komodia. Komodia's code allowed Superfish to falsely represent that it had authority to decrypt the secure information being diverted through its proxy. Thus, when VisualDiscovery was preloaded on a computer, an additional unrestricted, self-signing root-certificate authority was also installed into the Windows operating system.

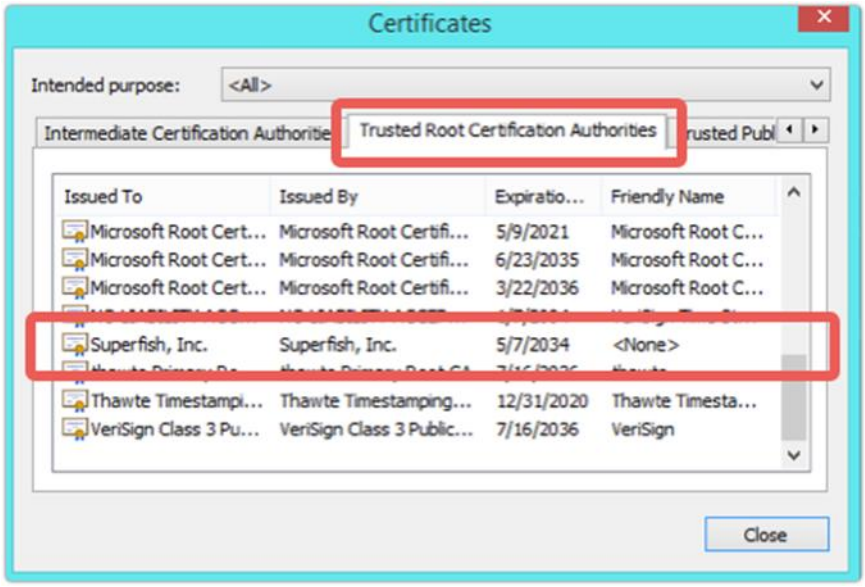
56. Komodia is a privately-held Israeli company founded by a former member of the Israeli Defense Force's Intelligence Core. Komodia's products have been criticized as being "hugely intrusive and poorly protected."[22] Security researchers investigating Komodia's primary products "found

[21] Matthias Gelbmann, *Comodo has become the most widely used SSL certificate authority*, Feb. 17, 2015, W3Techs, http://w3techs.com/blog/entry/comodo_has_become_the_most_widely_used_ssl_certificate_authority (last visited Sept. 30, 2015).

[22] Thomas Fox-Brewster, *The Company Behind Lenovo's Dangerous Superfish Tech Claims It's Under Attack*, Feb. 20, 2015, Forbes, http://www.forbes.com/sites/thomasbrewster/2015/02/20/komodia-lenovo-superfish-ddos/ (last visited Sept. 29, 2015).

numerous implementation problems" and "poor security design."[23] "In other words, the entire Komodia engine is a hopelessly broken implementation of public key infrastructure."[24]

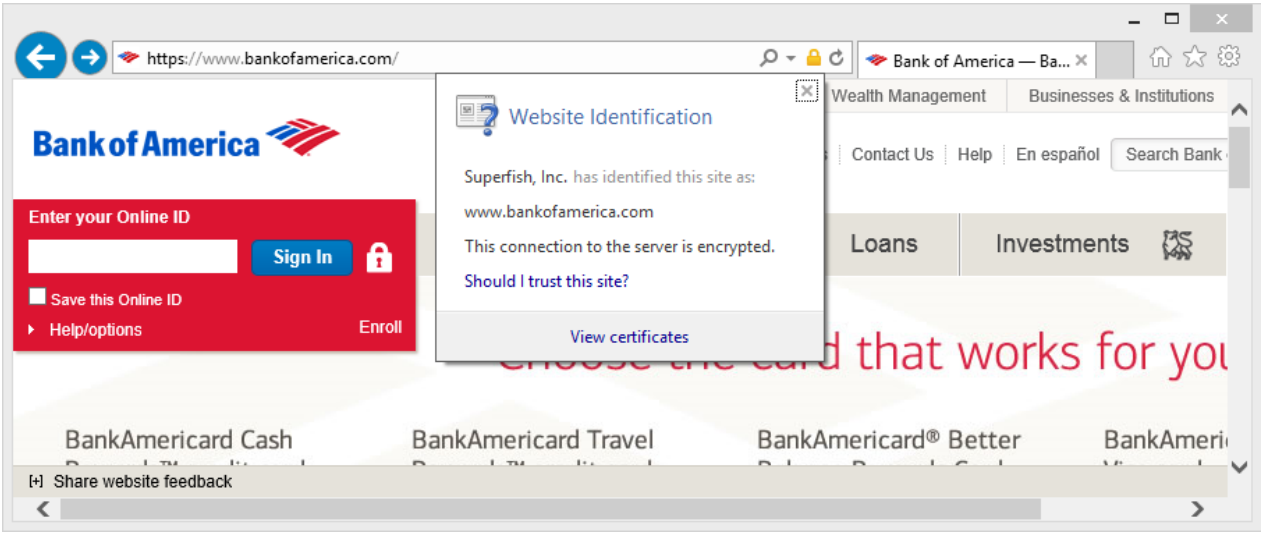
57. Komodia's technology allowed VisualDiscovery to insert the root-certificate authority into the list of trusted root-certificate authorities, and upon installation, allowed Superfish to impersonate any SSL-enabled site. Specifically, the technology – touted by Komodia as the "SSL hijacker"[25] – allowed Superfish to access data encrypted using SSL protocols and perform on the fly decryption. Essentially, Superfish was able to vouch for itself as a trusted root-certificate authority and as a trusted proxy:

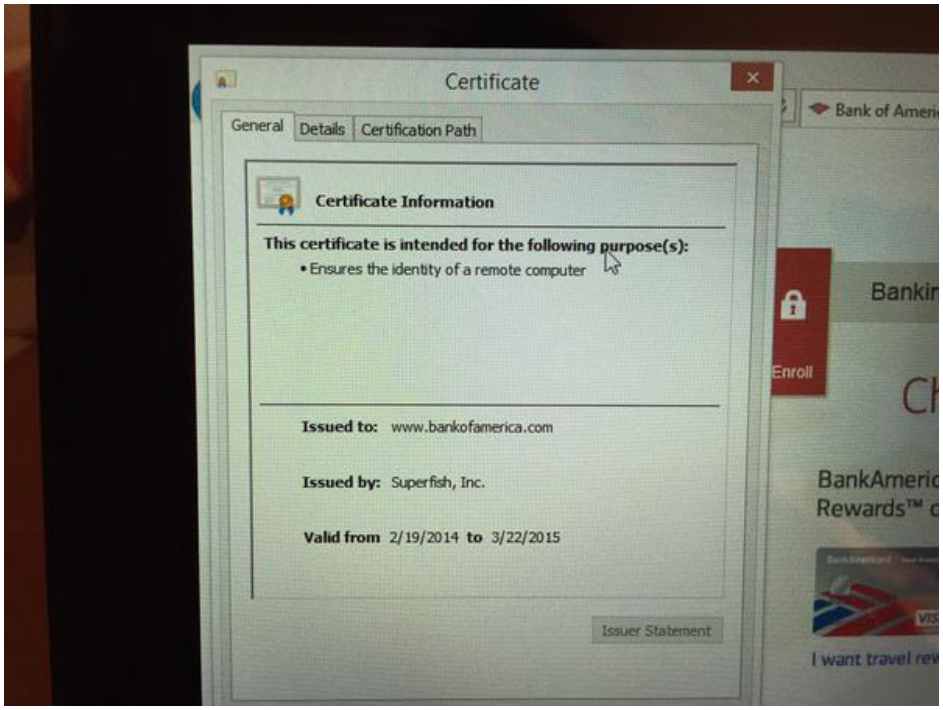


58. VisualDiscovery-generated digital certificates imitated the certificates of the actual encrypted websites Superfish intercepted and used them via its proxy to deliver content from the Superfish server over the same apparent domain, without revealing what was done. Because the digital certificates used by Superfish were signed by its own certificate authority, the browser did not have to

[23] Ryu Connor, *The Rest of the Story: Komodia, Lenovo, and Superfish*, Feb. 23, 2015, TechReport.com, http://techreport.com/news/27849/the-rest-of-the-story-komodia-lenovo-and-superfish (last visited Sept. 29, 2015).
[24] *Id.*
[25] "Komodia's SSL Decoder/Digestor." Komodia, http://www.komodia.com/products/komodias-ssl-decoderdigestor (last visited Sept. 11, 2015).

display any warnings that the traffic was being tampered with. It appeared that Superfish was the root certificate authority for all the websites visited and allowed the Superfish proxy to intercept an encrypted SSL connection, decrypt it using its own private key, and then re-encrypt again:





59. The operation of VisualDiscovery significantly degraded the performance of the Lenovo computers on which it was installed in several different, material ways. VisualDiscovery increased CPU usage, which increased power consumption. For laptop computers on which it was installed (and all of

the affected Lenovo computers were laptop), the increased CPU usage and power consumption decreased battery life, both in terms of the lifespan of the battery (number of times it could be recharged before being replaced) and the number of hours that the laptop could operate on a single charge. Furthermore, when VisualDiscovery was operational, [redacted]. It also caused certain webpages to fail to load correctly or not load at all.

60. Aside from the performance, privacy and ethical issues that the operation of VisualDiscovery raises, there are security issues as well. Unlike other legitimate certificate authorities, where the private key is secret and not available to the public, the private key for the VisualDiscovery certificate authority is visible in the software itself because it was never properly secured in accordance with certificate authority protocols.[26]

61. To make matters worse, the private key for the VisualDiscovery certificate authority is the same for every single computer on which the program is loaded, and it is protected by a very weak password that is also visible in the software itself and is also the same for every single computer.

62. Not surprisingly, when the Lenovo/Superfish controversy became public in late February 2015, it took computer researchers less than an hour to find Superfish's private key and figure out the password for it.[27] The password – "komodia" – proved "laughably easy to bypass."[28]

63. With this now widely-available information, anyone could extract a Superfish certificate and private key, issue his or her own certificate, and via Superfish, it would be trusted by the browser and, thus, by the Lenovo user. Even if the certificate was invalid, Superfish's certificate authority would have the ability to make the certificate valid.[29] Indeed, over 1,600 cases have been discovered in

[26] *See Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates*, CA/Browser Forum, Apr. 16, 2015, https://cabforum.org/wp-content/uploads/CAB-Forum-BR-1.3.0.pdf (last visited Sept. 28, 2015).

[27] Robert Graham, *Extracting the SuperFish certificate*, Errata Security, Feb. 19, 2015, http://blog.erratasec.com/2015/02/extracting-superfish-certificate.html#.Ve9lIk10yUk (last visited Sept. 28, 2015).

[28] http://arstechnica.com/security/2015/02/ssl-hijacker-behind-superfish-debacle-imperils-big-number-of-users/ (Last visited Nov. 6, 2015).

[29] Filippo Valsorda, *Komodia/Superfish SSL Validation is Broken*, Feb. 20, 2015, https://blog.filippo.io/komodia-superfish-ssl-validation-is-broken/ (last visited Sept. 28, 2015).

Superfish-Komodia attacks using invalid certificates, which were made valid by the Superfish certificate authority.[30]

64. Stated more simply, with the private key and password, a hacker with access to someone's wireless network or a shared public wireless network, could hijack a Lenovo computer with VisualDiscovery installed on it and, without the user's knowledge, collect whatever information the user was transmitting at the time, including personal financial information, passwords or other confidential information.

III. Lenovo and Superfish Partner to Load VisualDiscovery on Lenovo's Consumer PC Models and Share in any Revenues

65. In early 2014, Superfish and Lenovo executives began discussions about partnering to load VisualDiscovery onto certain Lenovo computers sold to consumers in the United States and elsewhere and then sharing in the revenues flowing from that arrangement.

66. [redacted]

67. [redacted]

68. [redacted]

[30] GranTorinoGuy, *Over 1,600 Domains Discovered in Superfish-Komodia MitM Attacks Using Invalid HTTPS Security Certificates*, Mar. 26, 2015, PC Overdose, http://www.pcoverdose.com/1600-domains-superfish-komodia-mitm-attacks-invalid-https-certificates.php (last visited Sept. 28, 2015).

[redacted]

69. [redacted] That description said nothing, however, about the security, privacy, or performance implications discussed in this Complaint, and did not take reasonable steps to make clear to a reasonable consumer that VisualDiscovery was separately installed and running on the computer (as opposed to being incorporated within a search engine or web browser). Consequently, the reasonable consumer was not fairly put on notice of the existence of VisualDiscovery on his or her computer, let alone the implications of its existence and operation.

70. [redacted]

71. The early discussions between Lenovo and Superfish, which included demonstrations of the operation of VisualDiscovery, involved a number of senior Lenovo executives, some of whom expressed concerns about the program. These Lenovo executives included: Mark Cohen, Vice President of Cloud, Contextual Computing and Software Ecosystem; Dave Higgins, Vice President of Software Development; Jim Hunt, Executive Director of Software Development; and Feng Lee, Director of Worldwide Consumer and SMB (small to mid-size business) Software.

72. Lenovo and Superfish completed their negotiations and formalized their agreement in June 2014. The agreement was structured as a business partnership under which Superfish would

provide the software (VisualDiscovery) and Lenovo would provide the hardware (43 different Lenovo PC consumer models) and the two companies would then share in any revenues that flowed from the partnership.

73. [redacted]

74. [redacted]

75. [redacted]

76. Lenovo did in fact test and evaluate VisualDiscovery prior to it being loaded on any Lenovo computers and found that it did not satisfy Lenovo's acceptance criteria because certain features of the program "abused SSL connections."[31]

77. SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a computer user's browser. This link ensures that the data transmitted between the server and the browser remains private and intact.[32] The fact that VisualDiscovery was interfering with the ability of Lenovo's future customers to use the internet securely should have been a red flag (along with the Komodia-supplied code) for Lenovo. But, "[r]ather

[31] Simon Phipps, *Lenovo: 'We Were as Surprised as You"*, Feb. 20, 2015, InfoWorld, http://www.infoworld.com/article/2886959/laptop-computers/are-you-buying-risk-along-with-your-laptop.html (last visited Sept. 29, 2015).

[32] https://www.digicert.com/ssl.htm (last visited Sept. 29, 2015).

than dropping Superfish like a rock, which is what you're supposed to do when a software partner compromises your customers' security," Lenovo instead simply asked Superfish to remove some of the features from the program.[33]

78. Superfish thereafter provided Lenovo with a revised version of VisualDiscovery and assured Lenovo that the problems Lenovo had identified in the earlier version had been resolved.[34] But, contrary to Lenovo's own protocols and the Lenovo/Superfish partnership agreement, which required Lenovo to test and evaluate the program all over again, Lenovo did not do so. Instead, Lenovo simply accepted Superfish's assurance at face value.

79. [redacted]

80. Nevertheless, around August 2014, Lenovo began shipping hundreds of thousands of computers to consumers in the United States with VisualDiscovery hidden away deep within the operating system.[35]

81. The Lenovo computer models on which VisualDiscovery was installed include the following:

G Series:	G410, G510, G710, G40-70, G50-70, G40-30, G50-30, G40-45, G50-45
U Series:	U330P, U430P, U330Touch, U430Touch, U530Touch
Y Series:	Y430P, Y40-70, Y50-70
Z Series:	Z40-75, Z50-75, Z40-70, Z50-70
S Series:	S310, S410, S40-70, S415, S415Touch, S20-30, S20-30Touch
Flex Series:	Flex2 14D, Flex2 15D, Flex2 14, Flex2 15, Flex2 14(BTM), Flex2 15(BTM), Flex 10
MIIX Series:	MIIX2-8, MIIX2-10, MIIX2-11

[33] David Auerbach, *Are Lenovo and Superfish Evil or Incompetent*, Feb. 24, 2015, Slate, http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_the_result_of_evil_or_incompetence.html (last visited Sept. 29, 2015).
[34] Phipps, *supra*.
[35] *Id*.

YOGA Series: YOGA2Pro-13, YOGA2-13, YOGA2-11BTM, YOGA2-11HSW

E Series: E10-20

82. While Lenovo later claimed to be surprised by the problems created by VisualDiscovery, the facts indicate that Lenovo knew that the program would be unpopular and problematic even before it was shipped. In fact, Lenovo affirmatively undertook significant efforts to ensure that VisualDiscovery was not going to be discovered and threaten the future revenue stream Lenovo had partnered with Superfish to receive.

83. For computers sold in the United States, Lenovo usually lists on its website the third-party software that will come installed on each computer under the "Tech Specs" description for each model. Contrary to its usual custom and practice, however, VisualDiscovery was not identified anywhere on Lenovo's website and a prospective purchaser of a Lenovo computer would have no way of knowing that the program was going to be pre-installed on the computer. [redacted]

84. Lenovo was also selective in the computer models that VisualDiscovery would be installed on. All 43 of the Lenovo computer models that were sold in the United States with the program installed were models marketed and sold primarily to consumers. Lenovo carefully avoided installing VisualDiscovery on any of its computer models that were marketed and sold primarily to businesses and professionals, like the ThinkPad line of notebook computers. As one computer security expert noted, "[t]hey rely upon the fact that unsophisticated users don't know how to get rid of it, and will therefore endure the ads."[36]

85. For those computers models on which VisualDiscovery was installed, the manner of installation by Lenovo all but ensured that the program would not be detected by either the user or any internet security and antivirus programs running on the computer. VisualDiscovery was buried "in the lowest level of a computer's operating system, precisely where customers and antivirus products would

[36] Todd Haselton, *Lenovo Responds to "Superfish" Report, Says Malware is no Longer Active,* Feb. 19, 2015, TechnoBuffalo, http://www.technobuffalo.com/2015/02/19/lenovo-responds-to-superfish-report-says-malware-is-no-longer-active/ (last visited Sept. 30, 2015).

never detect it."[37]

86. McAfee, a leading antivirus vendor whose program was preinstalled on many of the Lenovo computers that contained VisualDiscovery, was unable to detect the program for more than five months and only discovered it after the controversy went public in February 2015. The same is true for Symantec, maker of the popular Norton AntiVirus, and Windows, maker of Windows Defender, a free program that operates on computers by default when a user has not activated any other antivirus program.

87. And finally, while it was operational, Lenovo only disclosed VisualDiscovery to users by way of a one-time small pop-up window that appeared during an internet search session and that a user would need to click in one particular spot in order to disable (but not remove) the program. The pop-up did not contain any detailed description of the program, looked similar to many other pop-up ads that appear on many web pages, and if the user simply clicked on the close icon [x] or anywhere outside the pop-up window, the window would close and the user was deemed to have accepted the program for all future purposes. The default for the program was opt-in, not opt-out:

[37] Nicole Perlroth, *Lenovo and Superfish Penetrate the Heart of a Computer's Security*, Feb. 22, 2015, NY Times, http://bits.blogs.nytimes.com/2015/02/22/lenovo-and-superfish-penetrate-the-heart-of-a-computers-security/ (last visited Aug. 26, 2015).

88. An example of the pop-up window appears above. Although there are no documents or public comments from a consumer praising VisualDiscovery, and the program is almost universally disliked, the opt-out rate, according to one internal Superfish document, appears to have averaged only about 2.2 percent. This low opt-out rate is attributable to the misleading design and functionality of the pop-up window.

89. The opt-out button in the pop-up frequently would not work even when clicked. While VisualDiscovery was operational, consumers repeatedly complained that they had tried to opt out, but continued to receive VisualDiscovery ads while browsing the internet: "Disable function fails. Please provide removal instructions;" "can't get rid of your pop-up. nothing works. very bad;" and "I find it very annoying and intrusive and I don't like that fact that no matter how many times I click opt out or disable, your product still keeps invading my browsing."

90. Consumer complaints about the operation of VisualDiscovery and, more generally, about significant performance issues with the Lenovo computers on which the program was installed, began almost immediately after Lenovo started shipping the computers in August 2014. In mid-September 2014, Lenovo received a complaint from an IT manager at a major bank that had purchased several Lenovo computers on which VisualDiscovery was installed. The IT manager complained that VisualDiscovery was interfering with encrypted sites and that it was intercepting secure communications by inserting a fake root certificate that effectively created a MitM attack.

91. [redacted]

92. Lenovo claims that after it received the complaint described in the preceding paragraph, it instructed Superfish to disable the HTTPS functionality of VisualDiscovery at the server level and that Superfish did so. According to Lenovo, once this occurred, VisualDiscovery would not work when an HTTPS site was visited, even though the self-signing root certificates (with their security risks) remained on users' Lenovo computers. Lenovo took no other action with respect to the program and did not even consider terminating its relationship with Superfish at that time.

93. According to Lenovo, Superfish then designed a new version of VisualDiscovery that would not operate on HTTPS sites and did not contain a self-signed root certificate. This version started to be loaded onto Lenovo computers in November 2014. While this release removed one of the security flaws in VisualDiscovery, it did not address any of the other issues with the program that have been alleged in this Complaint.

94. In October 2014, [redacted]

95. The customer complaints continued unabated and grew in number as more and more of the computers were shipped. Consumers complained that VisualDiscovery interfered with watching videos online, caused the computers to run slow, blocked or slowed connections to certain websites, and caused security issues. None of these complaints should have been surprising to Lenovo, which knew, [redacted]

96. [redacted]

97. As consumer complaints escalated and became more public throughout the Fall of 2014, Lenovo executives internally began to question whether VisualDiscovery should remain on Lenovo

computers. By November 2014, Lenovo's Chief Quality Officer was considering dropping the program. Superfish's executives assured Lenovo that the consumer complaints were unfounded and Lenovo did nothing as a result.

98. During those same conversations, Superfish's CEO suggested to Lenovo that the way to reduce consumer complaints and bad press was not to remove VisualDiscovery, but rather simply to change the name of the program since VisualDiscovery was becoming publicly known, and changing the name would prevent consumers from searching either their computer or the internet by the VisualDiscovery name.

99. Lenovo and Superfish's conspiracy of silence about VisualDiscovery began to unravel in January 2015 when Peter Horne, an Australian computer technology expert purchased a Lenovo computer on which the program was installed. Mr. Horne's Lenovo computer was running two different antivirus programs, but neither flagged VisualDiscovery. Instead, Mr. Horne saw that his internet traffic was being redirected through a different website and used this information and his expertise to trace the problem back to VisualDiscovery and then to Superfish.[38]

100. Mr. Horne conducted further research, including inspecting multiple Lenovo computers in multiple locations, to determine that the issue was widespread. He also investigated Superfish and what VisualDiscovery was doing to the Lenovo computers on which it was installed.[39] Mr. Horne concluded that VisualDiscovery was malware that compromised any computer on which it was installed and contacted Lenovo directly to be sure that they knew about the security issue created by the program. The Lenovo employee Mr. Horne spoke with stated that he must be mistaken because "Lenovo doesn't distribute Malware." Mr. Horne asked to speak to a Lenovo product manager, but he got no response. After waiting several weeks in vain for a response from Lenovo, Mr. Horne contacted a technology reporter at the New York Times, Nicole Perlroth, who investigated and then broke the story on February

[38] Nicole Perlroth, *Lenovo and Superfish Penetrate the Heart of a Computer's Security*, Feb. 22, 2015, NY Times, http://bits.blogs.nytimes.com/2015/02/22/lenovo-and-superfish-penetrate-the-heart-of-a-computers-security/ (last visited Aug. 26, 2015).

[39] *Id.*

19, 2015.[40]

101. Mr. Horne was not the only computer technology expert who had concerns about what Lenovo and Superfish were doing during this period. In late January 2015, a user posted a detailed description of Superfish and its problems to a Lenovo forum."[41] The message from this user was part of a message thread initiated in November 2014 and titled "Potentially Unwanted Program – Superfish VisualDiscovery".[42] Within this forum, various users noted that VisualDiscovery was part of the bundled software that came pre-installed on Lenovo laptops and that the program caused problems with laptop web sockets. In relevant part, the late January message states:

> [T]his is more serious than just a simple socket messup [*sic*].
>
> **Superfish** Inc aka **VisualDiscovery** . . . application will hijack ALL your secure webconnections (SSL/TLS) by using self signed root certificate authority, making it look legitimate to the browser[.] . . .
>
> Here's an example of my connection to a bank, which looked OK to browser but certificate obviously has been tampered with allowing Superfish to collect all data une[n]crypted.
>
> A bluntant [sic] man-in-the-middle attack malware breaking any privacy laws.
>
> I have requested return of the laptop and refund as I find it unbelievable that [a] manufacturer as Lenovo would facilitate such applications pre-bundled with new laptops.[43]

While Lenovo generally responded quickly to user messages posted on Lenovo user forums, in this instance, Lenovo did not respond until February 19, after the New York Times story had broken. [44]

---

[40] Patricia Seybold, *Patty's Pioneer, Peter Horne, Exposes Lenovo Security Risk*, Feb. 27, 2015, http://www.customers.com/forum/pattys-pioneer-peter-horne-exposes-lenovo-security-risk/ (last visited Oct. 1, 2015).

[41] David Auerbach, *You Had One Job, Lenovo*, Feb. 20, 2015, Slate, http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_why_it_s_one_of_the_worst_consumer_computing_screw.html (last visited Aug. 27, 2015).

[42] https://forums.lenovo.com/t5/Security-Malware/Potentially-Unwanted-Program-Superfish-VisualDiscovery/td-p/1794457.

[43]https://forums.lenovo.com/t5/Security-Malware/Potentially-Unwanted-Program-Superfish-VisualDiscovery/m-p/1860408/highlight/true#M1697 (emphasis in original).

[44] https://forums.lenovo.com/t5/Security-Malware/Potentially-Unwanted-Program-Superfish-VisualDiscovery/td-p/1794457.

V. The Truth Emerges

102. On February 19, 2015, the New York Times and a number of other prominent publications released highly critical articles condemning Superfish, for its poorly designed and intrusive VisualDiscovery product, and Lenovo, for selling out its customers by agreeing to hide VisualDiscovery deep in Lenovo computers for money and without conducting due diligence.

103. The articles that day and in the days that followed, and every computer expert that was interviewed, universally condemned Lenovo and Superfish for what they had done, as demonstrated by the following examples:

- "Lenovo has not just injected ads in a wildly inappropriate manner, but engineered a massive security catastrophe for its user . . . Using a MITM [man-in-the-middle] certificate to inject ads was an amateurish design choice by Superfish. Lenovo's decision to ship this software was catastrophically irresponsible and an utter abuse of the trust their customers placed in them."[45]

- "When Lenovo preinstalled Superfish adware on its laptops, it betrayed its customers and sold out their security. It did it for no good reason, and it may not even have known what it was doing. I'm not sure which is scarier."[46]

- It's "quite possibly the single worst thing I have seen a manufacturer do to its customer base . . . I cannot overstate how evil this is."[47]

- "Computer maker Lenovo has been shipping laptops prepackaged with malware that makes you vulnerable to hackers – all for the sake of serving you advertisements . . . Besides taking up space in your Lenovo computer, the add-on is also dangerous because it undermines basic computer security protocols."[48]

- "Lenovo's Superfish security snafu blows up in its face – The preloaded Superfish adware does more than hijack website ads in a browser. It also exposes Lenovo owners to a simple but dangerous hack that could spell disaster."[49]

---

[45] Joseph Bonneau, *Lenovo is Breaking HTTPS Security on its Recent Laptops*, Feb. 19, 2015, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2015/02/further-evidence-lenovo-breaking-https-security-its-laptops (last visited Oct. 2, 2015).

[46] Auerbach, *You Had One Job, Lenovo*, *supra*.

[47] *Id*.

[48] Jose Pagliery, *Lenovo Slipped 'Superfish' Malware Into Laptops*, Feb. 19, 2015, CNN, http://money.cnn.com/2015/02/19/technology/security/lenovo-superfish/ (last visited Oct. 2, 2015).

[49] Seth Rosenblatt, *Lenovo's Superfish Security Snafu Blows Up in its Face*, Feb. 20, 2015, CNET, http://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware/ (last visited Oct. 2, 2015).

- "The Chinese computer-making giant Lenovo was inserting spyware – its defenders would call it adware – in its PCs. This software could track customers' every online move, intercept secure web sessions and render their computers vulnerable to hackers. The company buried its software in the lowest level of a PC's operating system, precisely where customers and antivirus products would never detect it, and had been siphoning data back to servers belonging to Superfish."[50]

- "Lenovo might have made one of the biggest mistakes in its history. By pre-installing software called 'Superfish' to get ads on screens it's peeved the entire privacy community, which has been aghast this morning on Twitter. There are serious security concerns about Lenovo's move too as attackers could take Superfish and use it to ensnare some unwitting web users."[51]

104. On February 20, 2015, the U.S. Department of Homeland Security took the extraordinary step of issuing an public alert advising consumers with a Lenovo computer on which VisualDiscovery was installed to remove the program immediately, explaining:

> In order to intercept encrypted communications (those using HTTPS), [VisualDiscovery] installs a trusted root CA certificate for Superfish. All browser-based encrypted traffic to the Internet is intercepted, decrypted, and re-encrypted to the user's browser by the application—a classic man-in-the-middle attack. . . . [W]ebsites, such as banking and email, can be spoofed without a warning from the browser.[52]

The alert cautioned that removal of the VisualDiscovery software was insufficient and that consumers with affected computers also needed to remove each and every fake certificate that resided in the root directory of the computer.

105. While the alert quoted above focused only on encrypted HTTPS traffic, the Lenovo security advisory issued that same day suggests that the same process was occurring with respect to HTTP traffic. Lenovo labeled the threat presented by VisualDiscovery as "high," its most severe rating.

---

[50] Perlroth, *Lenovo and Superfish Penetrate the Heart of a Computer's Security*, *supra*.

[51] Thomas Fox-Brewster, *How Lenovo's Superfish 'Malware' Works and What You Can Do to Kill It*, Feb. 19, 2015, Forbes, http://www.forbes.com/sites/thomasbrewster/2015/02/19/superfish-need-to-know/ (last visited Oct. 2, 2015).

[52] Department of Homeland Security, United States Computer Emergency Readiness Team, *Alert (TA15-051A), Lenovo Superfish Adware Vulnerable to HTTPS Spoofing*, Feb. 20, 2015, revised Feb. 24, 2015, https://www.us-cert.gov/ncas/alerts/TA15-051A (last visited Aug. 28, 2015).

In Lenovo's words, "SuperFish intercepts HTTP(S) traffic using a self-signed root certificate. This is stored in the local certificate store and provides a security concern."[53]

106. Lenovo and Superfish responded differently when the truth emerged; neither well. Superfish responded by denying that VisualDiscovery created any security risks for the computers on which it was installed while at the same time claiming that the security vulnerabilities that did exist on those computers were introduced unintentionally by a third party (Komodia). Superfish also claimed that it and Lenovo had done extensive security testing of VisualDiscovery before it was released and that its partnership with Lenovo was limited in scale.[54]

107. None of these statements by Superfish are true. While publicly denying any problem, Superfish's CEO was frantically telling his staff to "PLEASE CHANGE THE PASSWORD FIRST NOW!!!!!!!!!!!!!!!!!!!!!!" because "our master cert has been compromised. This should happen ASAP."

108. And the security vulnerabilities were not "introduced unintentionally" by Komodia, they were introduced purposefully and knowingly by Superfish. As one computer security expert noted, "Superfish catastrophically compromises the security of your entire machine. A software company cannot integrate an 'SSL hijacker' into its product without having some idea of what it's doing."[55]

109. Lenovo admitted that it did virtually no due diligence on VisualDiscovery before it was released and that its testing generally of third-party software was far less extensive than for its own software, directly refuting Superfish's claim that the two companies did extensive testing before VisualDiscovery was released. And finally, Superfish's partnership with Lenovo was not limited in scale. [redacted] and, even though the partnership only lasted about five months, they still managed to install the program on about 800,000 Lenovo computers sold in the United States.

[53] LENOVO, LENOVO SECURITY ADVISORY: LEN-2015-10, SUPERFISH VULNERABILITY, https://support.lenovo.com/us/en/product_security/superfish (last visited Aug. 28, 2015).
[54] Dan Goodin, *Superfish Doubles Down, Says HTTPS-busting Adware Poses No Security Risk,* ARS TECHNICA, Feb. 20, 2015, http://arstechnica.com/security/2015/02/superfish-doubles-down-says-https-busting-adware-poses-no-security-risk/ (last visited Aug. 28, 2015).
[55] Auerbach, *Are Lenovo and Superfish Evil or Incompetent, supra*.

110. Lenovo eventually issued a public apology, but its response otherwise has not been better than Superfish's. As an initial matter, Lenovo only came forward and made any public statements about VisualDiscovery after the story broke on February 19. Lenovo admits that due to ongoing consumer complaints about VisualDiscovery, it ordered Superfish to turn off the server connections in January and stopped installing the program on new computers at the same time. Lenovo should have gone public then and alerted existing Lenovo computer owners that there were performance and security issues associated with VisualDiscovery and that the program needed to be removed, but did not do so.

111. When Lenovo did finally go public, its statements about Superfish and VisualDiscovery were met with a great deal of skepticism. Lenovo first claimed that the only reason it installed VisualDiscovery on Lenovo computers was "to enhance our user experience" and that "[t]he original motivation for this was that the product team was being asked, 'can we do something to improve our consumer experience?'"[56] As more than one computer security expert noted, "[o]bviously, that wasn't the main motivation. Even harmless bloatware isn't installed to improve the customer experience, it's installed to make OEMs money. No PC OEM goes around making a big deal about all the bloatware that comes preloaded on their devices because pretty much everyone hates bloatware."[57]

112. What Lenovo has never explained is why, if VisualDiscovery was so beneficial to consumers and would "enhance" and "improve" the user experience, Lenovo hid it deep within the operating system, never disclosed VisualDiscovery anywhere on its website, and designed the program to be opt-out instead of opt-in. The truth, according to Lenovo, is that the sole purpose of the program was to make money for Lenovo and Superfish at the expense of Lenovo's customers.

113. Lenovo also claimed, again after the fact, that it did not start receiving complaints about VisualDiscovery until December 2014, and then promptly took action to address those complaints in January 2015.[58] This too is false. As discussed above, consumer complaints about VisualDiscovery,

---

[56] Nicole Perlroth, *Lenovo's Chief Technology Officer Discusses the Superfish Adware Fiasco*, Feb. 24, 2015, NY Times, http://bits.blogs.nytimes.com/2015/02/24/lenovos-chief-technology-officer-discusses-the-superfish-adware-fiasco/?_r=0 (last visited Oct. 2, 2015).

[57] Brad Reed, *Interview with Lenovo's CTO Will Scare Anyone Still Thinking of Buying a Lenovo Product*, Feb. 25, 2015, http://bgr.com/2015/02/25/lenovo-superfish-adware-scandal/ (last visited Oct. 2, 2015)

[58] Perlroth, *Lenovo's Chief Technology Officer Discusses the Superfish Adware Fiasco, supra.*

including the negative effects it was having on the Lenovo computers on which it was installed, began almost as soon as those computers started to be sold in September 2014, and increased in number and frequency as more and more Lenovo PCs entered the marketplace. Lenovo appears to have finally taken action in January 2015 because that is when computer experts started going public about the problems caused by VisualDiscovery and the Lenovo-Superfish relationship.

114. Lenovo claimed that VisualDiscovery was an opt-in program: "We make sure it's opt-in."[59] But, as discussed above, while Lenovo and Superfish originally contemplated that VisualDiscovery would be an opt-in program, by the time it was released, it was undisputedly an opt-out program, with the opt-out designed specifically to avoid triggering opt-outs, which it did for the most part.

115. Finally, while Lenovo conceded that it failed to conduct due diligence of VisualDiscovery before it was installed on Lenovo computers, it claimed that it was unaware of any security issues until February 2015 and only learned about Komodia's involvement with VisualDiscovery two months earlier.[60] In fact, Lenovo learned about the security issues in January, at the latest, [redacted], and knew before VisualDiscovery was installed on any Lenovo computers that the program "abused SSL connections." All Lenovo had to do at any point before it shipped a computer with VisualDiscovery installed was conduct an internet search of Komodia (and Superfish for that matter) to have understood who it was partnering with and what these companies were up to.

116. One computer security expert had this response to Lenovo's claim that it did not understand what security issues might be created by the operation of VisualDiscovery: "You absolutely have to be kidding me."[61] Lenovo is the largest computer company in the world and the notion that it did not know how the technology it was about to load on 20 million of its computers was implemented, particularly when that information was widely available on the internet, defies belief.

---

[59] *Id*.
[60] *Id*.
[61] Reed, *Interview with Lenovo's CTO Will Scare Anyone Still Thinking of Buying a Lenovo Product*, *supra*.

117. Since the truth emerged, Lenovo has severed its relationship with Superfish and worked with the large antivirus providers to provide automated tools to remove VisualDiscovery and the fake root certificates from Lenovo computers. On February 27, 2015, Lenovo promised to offer "a free 6-month subscription to McAfee LiveSafe service," but consumers would only know of this offer by independently learning of it and then would be required to visit www.lenovo.com to obtain relevant information about the service.[62] By visiting this website, however, the user has to consent to being tracked by cookies, web beacons, or "other technologies" of "Lenovo or its [unnamed] third-party vendors."[63]

118. On March 21, 2015, Lenovo issued an "Important Security Message" via the Lenovo Messenger advisory tool to users whose computers still contained the VisualDiscovery software. The message contained links to instructions on how to remove VisualDiscovery. However, Lenovo may not have designed the message to reach all users who purchased affected computers. Specifically, it is unclear whether Lenovo sent messages to users who had removed the VisualDiscovery software but may not have removed each and every self-signed root certificate.

119. More than a few computer security experts have argued that completely wiping the computer's memory and reinstalling a non-Lenovo "vanilla" version of Windows is the only way to ensure that the VisualDiscovery-caused security problem is completely solved and that the Lenovo computers on which the program was installed are returned to the user's "full control."[64]

120. These concerns are well-founded. *Ars Technica* reports that Lenovo's official Superfish removal tool leaves behind several files related to VisualDiscovery—"VisualDiscovery.exe" and "SuperfishCert.dll"—and a VisualDiscovery registry setting.[65]

---

[62] LENOVO, INFORMATION ON FREE MCAFEE SUBSCRIPTION FOR LENOVO CUSTOMERS WITH SUPERFISH PRELOAD, https://support.lenovo.com/us/en/mcafeesubscription.

[63] *See* LENOVO, PRIVACY DETAILS, http://www.lenovo.com/privacy/details/us/en/.

[64] Andrew Cunningham, *Save Yourself from Your OEM's Bad Decisions with a Clean Install of Windows 8.1*, ARS TECHNICA, Feb. 19, 2015, http://arstechnica.com/gadgets/2015/ 02/save-yourself-from-your-oems-bad-decisions-with-a-clean-install-of-windows-8-1/1/ (last viewed Aug. 28, 2015).

[65] Dan Goodin, *Two Weeks On, Superfish Debacle Still Causing Pain for Some Lenovo Customers*, ARS TECHNICA, Mar. 6, 2015, http://arstechnica.com/security/2015/03/two-weeks-on-superfish-debacle-still-causing-pain-for-some-lenovo-customers/ (last visited Aug. 28, 2015).

APPLICABLE LAW

121. Lenovo sells its products either directly to the consumer or indirectly through a store or online provider. [redacted]

122. Lenovo's direct sales to consumers are governed by a uniform sales agreement that includes a New York choice-of-law provision. Therefore, when the sale is direct from Lenovo to the consumer, New York law applies.

123. Additionally, the June 2014 agreement between Superfish and Lenovo [redacted]

124. California law applies to Jessica Bennett and Rhonda Estrella's claims and all indirect purchasers' claims because Bennett, Estrella and all other indirect purchasers are intended third-party beneficiaries of the agreement between Superfish and Lenovo, [redacted]

125. The agreement contains a number of provisions that [redacted]

126. [redacted]

CLASS ACTION ALLEGATIONS

127. Plaintiffs incorporate by reference all the above allegations as if fully set forth herein.

128. Plaintiffs bring this action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of themselves and the following classes:

Direct Purchaser Class (represented by Richard Krause, Robert Ravencamp and Vincent Wong)

All persons who purchased one or more Lenovo computer models, on which VisualDiscovery was installed, in the United States directly from Lenovo.

Indirect Purchaser Class (represented by Jessica Bennett, Rhonda Estrella and John Whittle)

All persons who purchased one or more Lenovo computer models, on which VisualDiscovery was installed, in the United States from someone other than Lenovo.

California Class (represented by Jessica Bennett and Rhonda Estrella)

All persons who purchased one or more Lenovo computer models, on which VisualDiscovery was installed, in California.

New York Class (represented by Vincent Wong)

All persons who purchased one or more Lenovo computer models, on which VisualDiscovery was installed, in New York.

129. Excluded from the proposed Classes are governmental entities, Defendants, Defendants' affiliates and subsidiaries, Defendants' current or former employees, officers, directors, agents, representatives, and their family members, and the members of this Court and its staff.

130. Plaintiffs do not know the exact size or identities of the members of the proposed Classes, since such information is in the exclusive control of Lenovo. Plaintiffs believe that the Classes encompass hundreds of thousands of individuals whose identities can be readily ascertained from Defendants' books and records as well as third-party retailers. Therefore, the proposed Classes are so numerous that joinder of all members is impracticable.

131. Plaintiffs believe the amount in controversy exceeds $5 million.

132. All members of the proposed Classes have been subject to and affected by the same conduct. All purchased Lenovo computer models on which VisualDiscovery was preinstalled.

133. There are questions of law and fact common to the Classes that predominate over any questions affecting only individual members of the Classes. These questions include, but are not limited to the following:

a. Whether Defendants failed to disclose, inadequately disclosed, and concealed the installation of VisualDiscovery;

b. Whether Defendants had a duty to disclose the installation of VisualDiscovery;

c. Whether Defendants violated the Computer Fraud and Abuse Act, 18 U.S.C. §1030, et seq.;

d. Whether Defendants violated the Electronic Communications Privacy Act, 18 U.S.C. § 2512, et seq.;

e. Whether Superfish violated the Wiretap Act, 28 U.S.C. § 2510, et seq.;

f. Whether Defendants violated California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, et seq.;

g. Whether Lenovo violated California's Consumer Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq.;

h. Whether Defendants violated California's Computer Crime Law, Cal. Penal Code § 502, et seq.;

i. Whether Defendants violated California's Consumer Protection Against California's Computer Spyware Act, Cal. Bus. & Prof. Code §§ 22947, et seq.;

j. Whether Defendants violated California's Invasion Of Privacy Act, Cal. Penal Code § 630, et seq.;

k. Whether Defendants' acts constitute trespass and/or negligence under California and New York law;

l. Whether Defendants violated the New York Deceptive Acts & Practices Statute, N.Y. Gen. Bus. Law § 349;

m. Whether the above practices caused Class members to suffer injury; and

n. The proper measure of damages, restitution, or other appropriate relief.

134. The claims of the individually named Plaintiffs are typical of the claims of the proposed Classes and do not conflict with the interests of any other members of the proposed Classes.

135. The individually named Plaintiffs will fairly and adequately represent the interests of the respective Classes. They are committed to the vigorous prosecution of the Classes' claims and have retained and the Court has appointed attorneys who are qualified to pursue this litigation and have experience in class actions – in particular, consumer protection actions.

136. A class action is superior to other available methods for fair and efficient adjudication of this controversy. The damages suffered by individual Class members are small compared to the expense and burden of individual prosecution of this litigation. Individual plaintiffs may lack the financial resources to vigorously prosecute a lawsuit against Defendants to recover damages stemming from Defendants' unfair and unlawful practices.

137. This putative class action meets the requirements of Fed. R. Civ. P. 23(b)(3).

CLAIMS FOR RELIEF

COUNT I

COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. §1030 et seq.

(on behalf of Plaintiffs, the Direct and Indirect Purchaser Classes against Defendants Lenovo and Superfish)

138. Plaintiffs reallege and incorporate by reference all of the preceding paragraphs.

139. Plaintiffs bring this federal claim on behalf of themselves and the direct and indirect purchaser classes against Lenovo and Superfish.

140. The Consumer Fraud and Abuse Act (CFAA) establishes a private cause of action against a person who "knowingly accessed a computer without authorization or exceeding authorized access," and whose prohibited access results in damage or loss in excess of $5,000. *See* 18 U.S.C. § 1030(g), *referencing* § 1030(c)(4)(A)(i)(I); *see also* § 1030(a).

141. Specifically, the CFAA establishes liability against whoever:

a. "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer[,]" *id.* § 1030(a)(2)(C);

b. "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer[,]" *id.* § 1030(a)(5)(A);

c. "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage[,]" *id.* § 1030(a)(5)(B);

d. "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss[,]" *id.* § 1030(a)(5)(C);

e. "knowingly and with intent to defraud traffics (as defined in [18 U.S.C.] section 1029) in any password or similar information through which a computer may be accessed without authorization, if . . . such trafficking affects interstate or foreign commerce[,]" *id.* § 1030(a)(6)(A); or

f. "conspired to commit or attempts to commit an offense under subsection (a) of this section[,]" *id.* § 1030(b).

142. The CFAA defines "traffic" to mean "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of[.]" *Id.* §§ 1029(e)(5), 1030(a)(6)(A).

143. A "protected computer" is defined, in relevant part, as a computer "which is used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B).

144. Authorization is not statutorily defined, but "exceeds authorized access" is defined as "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.* § 1030(e)(6).

145. "Loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

146. Damage is defined as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

147. Plaintiffs' and the Class members' computers are used in or affect interstate and foreign commerce and communication, including through contact and communication with Internet websites, and are "protected" computers.

148. Through VisualDiscovery, Superfish intentionally accessed Plaintiffs' and the Class members' protected computers without authorization, or exceeded the authorization provided by Plaintiffs and the Class members, and thereby obtained information from such protected computers, in violation of 18 U.S.C. § 1030(a)(2)(C).

149. Through VisualDiscovery, Superfish intentionally accessed Plaintiffs' and Class members computers without authorization or exceeded authorized access and as a result caused a loss to Plaintiffs and Class members during a one-year period aggregating at least $5,000 in value, in violation of the CFAA.

150. Superfish caused Plaintiffs' and Class members' damages or loss in excess of $5,000 in the aggregate during a one-year period. This includes Plaintiff John Whittle, who used a Lenovo computer pre-installed with Superfish (a qualifying protected computer) for his income tax preparation business. Plaintiff Whittle suffered damages and losses to his business as a result of computer performance issues and suspected privacy intrusions caused by VisualDiscovery. The revenue lost, costs incurred, and consequential damages suffered because of interruption of service immediately before the federal and state income tax deadline of April 15, 2015, exceeds $5,000. Additionally, Plaintiff Whittle and Class members suffered diminished security and integrity of their computers, as well as their time, labor and money spent to investigate and remove the intrusive and dangerous VisualDiscovery program, the slower performance of their computers, the loss of business and personal opportunities and good will, the loss of time spent viewing and navigating away from sites and images to which they were redirected, and the costs of replacing affected computers that were no longer trustworthy as a result of the security risks and vulnerability caused by the installation and operation of the VisualDiscovery and the diminished value of their computers as a result of the installation of VisualDiscovery.

151. By installing and operating VisualDiscovery, which accessed, installed, and reconfigured the affected computers' essential operating components, including the SSL/TLS security protocol,

Defendants knowingly transmitted "a program, information, code, or command . . . to a protected computer" and, as a result of that conduct, intentionally caused damage without authorization to the affected protected computers, in violation of 18 U.S.C. § 1030(a)(5)(A).

152. Through VisualDiscovery, Superfish intentionally accessed a protected computer without authorization, and as a result of that conduct, recklessly caused damage to the affected computers, in violation of 18 U.S.C. § 1030(a)(5)(B).

153. Through VisualDiscovery, Superfish intentionally accessed protected computers without authorization, and as a result of that conduct, caused damage and loss to the affected computers in violation of 18 U.S.C. § 1030(a)(5)(C).

154. As indicated by the agreement between Lenovo and Superfish to preinstall VisualDiscovery on the affected computers, and Defendants' conduct as described herein, Defendants Lenovo and Superfish "conspired to commit . . . an offense" under the CFAA in violation of 18 U.S.C. § 1030(b).

155. Defendants' design, installation, and operation of VisualDiscovery, in particular its ability to spoof secure websites and monitor all Internet traffic, constitutes an attempt and/or conspiracy to commit an offense under the CFAA in violation of 18 U.S.C. § 1030(b).

156. Defendants knowingly and intentionally exceeded and conspired to exceed their authorized access to the computers purchased by Plaintiffs and the Class members insofar as Plaintiffs and other Class members did not authorize or consent to Defendants' interception of Plaintiffs' communications through VisualDiscovery.

157. By exceeding their authorized access, Defendants obtained information—the intercepted communications that Plaintiffs and other Class members sought to transmit to secure websites, as well as URLs with search terms, among other communications described herein —from the Lenovo computers.

158. Defendants' actions caused damage to Plaintiffs and their computers by rendering the computers uniquely vulnerable to third-party hackers and other malicious actors who could take advantage of Visual Discovery's ability to act as a Certificate Authority to conceal their own interception of Plaintiffs' and other Class members communications.

159. Based on Defendants' violation of the CFAA, Plaintiff seeks recovery of economic damages and injunctive relief on behalf of themselves and Class members, and all other relief provided by 18 U.S.C. § 1030(g).

COUNT II

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. § 2512 (on behalf of Plaintiffs, the Direct and Indirect Purchaser Classes against Defendants Lenovo and Superfish)

160. Plaintiffs reallege and incorporate by reference all of the preceding paragraphs.

161. Plaintiffs bring this federal claim on behalf of themselves and the direct and indirect purchaser classes against Defendants Lenovo and Superfish.

162. VisualDiscovery is an electronic, mechanical or other device which is designed to be primarily useful for the purpose of surreptitious interception of electronic communications. As described above, VisualDiscovery surreptitiously intercepts URLs with search terms, among other electronic communications.

163. Defendants Lenovo and Superfish intentionally possessed, manufactured, sold, and/or assembled an electronic, mechanical or other device knowing, or having a reason to know, that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or electronic communications and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce. Defendants, or someone at their direction, sent and/or received VisualDiscovery pre-installed on Lenovo computers by means of the United States Postal Service or commercial mail carrier. *See* 18 U.S.C. § 2512(1)(a) & (b).

164. Plaintiffs and Class members are persons whose electronic communications are being intercepted, disclosed and/or intentionally used in violation of 18 U.S.C § 2512.

165. As a result of Defendants' wrongful conduct, Plaintiffs and Class members are entitled, under 18 U.S.C. § 2520, to the greater of the sum of (1) actual damages they suffered as a result of Defendants' conduct, or (2) statutory damages in an amount the greater of $10,000 or $100 per day for each day Defendants acted in violation of 18 U.S.C. § 2512. *See* 18 U.S.C. § 2520(c)(2).

COUNT III

VIOLATION OF THE WIRETAP ACT, 18 U.S.C. § 2510 et seq.

(on behalf of Plaintiffs, the Direct and Indirect Purchaser Classes against Defendant Superfish)

166. Plaintiffs reallege and incorporate by reference all of the preceding paragraphs.

167. Plaintiffs bring this federal claim on behalf of themselves and the direct and indirect purchaser classes against Defendant Superfish.

168. The Federal Wiretap Act, 18 U.S.C. § 2510 et seq., prohibits the interception of any wire, oral, or electronic communications. The statute confers a civil cause of action on "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

169. "Electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…" 18 U.S.C. § 2510(12).

170. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

171. "Contents" is defined as "includ[ing] any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

172. "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

173. Plaintiff and Class members are persons as defined under § 2510(6) of the Act.

174. VisualDiscovery is a device for purposes of the Wiretap Act because it is software used to intercept electronic communication.

175. Superfish, through its design, authorship, programming, knowing and intentional installation, activation, and/or other involvement with VisualDiscovery has intentionally intercepted, endeavored to intercept, and/or procured others to intercept or endeavor to intercept, electronic

communications as described herein, in violation of 18 U.S.C. § 2511(1)(a). This interception was acquired during transmission, as VisualDiscovery operated in real-time to acquire the content of Plaintiffs' and the Class members' electronic communications, in order to display advertisements.

176. The contents intercepted include information concerning the substance, purport, or meaning of that communication, including, but not limited to, usernames, passwords and other personal identification data submitted or received through websites, URLs containing a user's search terms, text associated with product images and the name of websites searched for or visited.

177. Plaintiffs' and the Class members' electronic communications were intercepted without their consent. Superfish was not the intended recipient of Plaintiffs' and the Class members' electronic communications. Superfish intercepted Plaintiffs' and the Class members' electronic communications for the unlawful and/or wrongful purpose of using their private information to create targeted advertisements for profit, without Class members' consent, and did so in reckless disregard of the computer security vulnerability and severe performance impairment VisualDiscovery created.

178. As a result, Plaintiffs and Class members have suffered harm and injury, including due to the interception and transmission of private and personal, confidential, and sensitive communications, content, and data, and also the degraded performance of their affected computers.

179. Plaintiffs and the Class have been damaged by the interception or disclosure of their communications in violation of the Wiretap Act, as described herein, and are thus entitled to preliminary, equitable, or declaratory relief; statutory and punitive damages; and reasonable attorney's fees and litigations costs reasonably incurred. 18 U.S.C. § 2520(b).

COUNT IV

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW

CAL. BUS. & PROF. CODE §§ 17200, *et seq.*

(on behalf of Plaintiffs, the Indirect Purchaser Class, and the California Class against Defendants Lenovo and Superfish)

180. Plaintiffs, the Indirect Purchaser Class, and the California Class incorporate by reference each preceding and succeeding paragraph as though fully set forth herein.

181. Plaintiffs bring this claim on behalf of themselves, the indirect purchaser class, and the California Class members against Lenovo and Superfish.

182. Lenovo's and Superfish's acts and practices, as alleged in this Complaint, constituted unlawful, unfair, and fraudulent business practices, in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq*.

183. Defendants' acts and practices constituted unlawful business practices in that they violated the Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq.*; the Computer Fraud & Abuse Act, 18 U.S.C. § 1030; the Electronic Communications Privacy Act, 18 U.S.C. § 2512; the Consumer Protection Against Spyware Act, Cal. Bus. & Prof. Code §§ 22947, *et seq.*; the California Computer Crime Law, Cal. Penal Code § 502; the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; the California Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.*; and constituted negligence and trespass to chattels under California common law.

184. Defendants' acts and practices also constituted unfair and fraudulent competition in violation of the Unfair Competition Law. *See* Cal. Bus. & Prof. Code §§ 17200, *et seq*. Lenovo's and Superfish's acts and practices were unfair in that (i) they were immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers; (ii) they harmed consumers in a manner far outweighing any legitimate utility of their conduct; (iii) the injury was not one that consumers reasonably could have avoided; (iv) they were contrary to legislatively declared and public policy; (v) they constituted knowing, intentional, and material misrepresentations of the purpose of VisualDiscovery and its access to Plaintiffs' and Class members' computers and private information; (vi) they were designed to and likely to deceive reasonable consumers, including Plaintiffs and Class members, because reasonable consumers would not anticipate that their computers would contain software that would impair the performance and battery life of the machines and put consumers' data privacy and security at risk; and (vii) they did deceive Plaintiffs and Class members, who relied on these misrepresentations in their purchase of Lenovo computers and who would not have purchased the computers or would have paid substantially less for them had Lenovo adequately disclosed the installation of and risks associated with VisualDiscovery.

185. As a direct and proximate result of Defendants' unlawful, unfair, and fraudulent business practices, Plaintiffs and Class members have suffered injury in fact and lost money or property; they bought computers that they otherwise would not have, overpaid for their computers, did not receive the benefit of their bargain, and their computers suffered a diminution in value during the time period in which VisualDiscovery was installed. In additional, Plaintiffs and Class members have incurred additional costs of hiring professionals to uninstall VisualDiscovery. Meanwhile, Lenovo has sold more computers than it otherwise could have while charging inflated prices and obtaining an upfront "slotting" fee from Superfish for each computer installed with VisualDiscovery, and Lenovo and Superfish have obtained advertising revenue through payments from VisualDiscovery's clients that they otherwise could not have, thereby unjustly enriching themselves.

186. Plaintiffs and the proposed California Class are entitled to equitable relief, including restitutionary disgorgement of all profits accruing to Defendants because of their unfair and deceptive practices, and such other orders as may be necessary to prevent the future use of these practices.

COUNT V

VIOLATIONS OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT

CAL. CIV. CODE §§ 1750, *et seq*.

(on behalf of Plaintiffs, the Indirect Purchaser Class, and the California Class Against Defendant Lenovo)

187. Plaintiffs, the Indirect Purchaser Class, and the California Class incorporate by reference each preceding and succeeding paragraph as though fully set forth herein.

188. Plaintiffs bring this claim on behalf of themselves, the Indirect Purchaser Class, and the California Class against Lenovo.

189. Plaintiffs and members of the Class are "consumers" under Cal. Civ. Code § 1761(d).

190. Lenovo is a "person" under Cal. Civ. Code § 1761(c).

191. The Lenovo computers at issue herein are "goods" under Cal. Civ. Code § 1761(a), and their sale to consumers constituted a transaction under § 1761(e).

192. Lenovo violated the Consumer Legal Remedies Act (CLRA), Cal. Civ. Code § 1770(a), thereby engaging in unfair methods of competition and unfair or deceptive acts and practices in

connection with a transaction, through concealing and failing to disclose prior to the sale of the affected computers that these computers were pre-installed with VisualDiscovery software and that this software impacted the performance of the computer and the privacy and security of users' data.

193. These facts were material to a reasonable purchaser of Lenovo computers because a reasonable purchaser would not anticipate that the computers would be installed with such software. These facts were also material because they negatively impacted the market value of Lenovo computers.

194. Lenovo had a duty to disclose the pre-installation of VisualDiscovery and its associated privacy risks and computer performance issues because Lenovo had exclusive knowledge of the pre-installation of VisualDiscovery, which was not known or reasonably knowable by Plaintiffs and the proposed Class; because it actively concealed the pre-installation from these purchasers; and because it made partial representations to new users by notifying them about VisualDiscovery on their web browsers, but at the same time suppressed the fact that VisualDiscovery violated users' privacy, exposed them to security risks, and had a negative impact on computer performance and battery life.

195. Through these fraudulent omissions, Lenovo represented that the computers had "sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities" that they did not have, in violation of Cal. Civ. Code § 1770(a)(5). Lenovo also represented that the computers were "of a particular standard, quality, or grade" that they were not, in violation of Cal. Civ. Code § 1770(a)(7).

196. Plaintiffs and Class members actually relied on these misrepresentations in purchasing their Lenovo computers.

197. As a direct and proximate result of Lenovo's conduct, Plaintiffs and Class members have suffered actual damages and lost money or property. Plaintiffs and Class members did not receive the benefit of their bargain, they have purchased computers that they otherwise would not have, and their computers suffered a diminution in value during the time period that VisualDiscovery was installed on them.

198. Plaintiffs and the proposed Class are entitled to equitable relief and a declaration that Lenovo's conduct violates the CLRA.

199. Plaintiffs have provided notice to Lenovo on behalf of themselves and potential class members; that notice period has expired; and thus Plaintiffs and the Class are entitled to actual damages

and costs and attorney fees pursuant to Cal. Civ. Code § 1780(d) and 1782(d). Plaintiffs and the Class are also entitled to punitive damages under Cal. Civ. Code § 1780(a)(4) because Lenovo's conduct was malicious, willful, reckless, wanton, fraudulent, and in bad faith.

COUNT VI

VIOLATIONS OF CALIFORNIA'S COMPUTER CRIME LAW

Cal. Penal Code § 502

(on behalf of Plaintiffs, the Indirect Purchaser Class, and the California Class Against Defendants Lenovo and Superfish)

200. Plaintiffs, the Indirect Purchaser Class, and the California Class incorporate by reference all allegations of the preceding and succeeding paragraphs as though fully set forth herein.

201. Plaintiffs bring this claim on behalf of themselves, the Indirect Purchaser Class and the California Class against Lenovo and Superfish.

202. VisualDiscovery is a "computer program or software" and "computer contaminant" under Cal. Penal Code § 502(b)(3) and (12). VisualDiscovery has "access" to Plaintiffs' and Class members' computers, computer systems, and computer networks under Cal. Penal Code § 502(b)(1). VisualDiscovery also collected "data" from Plaintiffs' and Class members' computers under Cal. Penal Code § 502(b)(8).

203. Superfish and Lenovo acted "without permission" under Cal. Penal Code 502 because Plaintiffs and Class members did not choose to install VisualDiscovery, but rather unknowingly purchased computers with VisualDiscovery software preinstalled. Furthermore, Superfish and Lenovo acted without permission because Plaintiffs and Class members were not given an opportunity to opt in to the software, but rather were given only a single and confusing opportunity to opt out of the software—and during this opt-out window, the functionality, privacy, and security problems of VisualDiscovery were not disclosed. Superfish and Lenovo also acted without permission because in some cases VisualDiscovery continued to run on Plaintiffs' and Class members' computers despite their opt out.

204. The California Computer Crime Law prohibits knowing and unauthorized access to computers. *See* Cal. Penal Code § 502. Through the knowing installation and operation of Visual

Discovery on Plaintiffs' and Class members' computers without permission, Superfish and Lenovo have violated the following provisions of the California Computer Crime Law:

205. Superfish accessed and used Plaintiffs' and Class members' data to wrongfully control and obtain data on their computers, in violation of Cal. Penal Code § 502(c)(1)-(2).

206. Superfish accessed and used data from Plaintiffs' and Class members' computers, in violation of Cal. Penal Code § 502(c)(3).

207. Lenovo provided and assisted in providing Superfish with a means of accessing Plaintiffs' and Class members' computers and violating the California Computer Crime Law, in violation of Cal. Penal Code § 502(c)(6).

208. Superfish accessed and Lenovo caused to be accessed Plaintiffs' and Class members' computers, in violation of Cal. Penal Code § 502(c)(7).

209. Superfish and Lenovo introduced VisualDiscovery, a computer contaminant, onto Plaintiffs' and Class members' computers, in violation of Cal. Penal Code § 502(c)(8).

210. Superfish used the internet domain names and profiles of other individuals, corporations, and entities through injecting code into https secure websites with false certificates, in violation of Cal. Penal Code § 502(c)(9).

211. As an actual and proximate result of Defendants' unlawful conduct under the California Computer Crime Law, Plaintiffs and Class members have been damaged in an amount to be determined at trial. Plaintiffs and Class members are entitled to compensatory damages, injunctive and other equitable relief, and attorney fees under Cal. Penal Code § 502(e)(1) and (2). Additionally, because Defendants willfully violated this statute with oppression, fraud, or malice under Cal. Civil Code §3294, Plaintiffs and Class members seek punitive and exemplary damages pursuant to Cal. Penal Code § 502(e)(4).

COUNT VII

VIOLATIONS OF CALIFORNIA'S CONSUMER PROTECTION AGAINST CALIFORNIA'S COMPUTER SPYWARE ACT

Cal. Bus. & Prof. Code §§ 22947, *et seq*.

(on behalf of Plaintiffs, the Indirect Purchaser Class, and the California Class Against Defendants Lenovo and Superfish)

212. Plaintiffs, the Indirect Purchaser Class, and the California Class incorporate by reference all allegations of the preceding and succeeding paragraphs as though fully set forth herein.

213. Plaintiffs bring this claim on behalf of themselves, the Indirect Purchaser Class, and the California Class against Defendants.

214. Plaintiffs are "authorized users" and "consumers" under Cal. Bus. & Prof. Code § 22947.1.

215. Lenovo and Superfish are not "authorized users" under Cal. Bus. & Prof. Code § 22917.1. "An 'authorized user' does not include a person or entity that has obtained authorization to use the computer solely through the use of an end user license agreement." *See id.*

216. VisualDiscovery is "computer software" under Cal. Bus. & Prof. Code § 22917.1. *Id.*

217. Damage under Cal. Bus. & Prof. Code § 22917.1 constitutes "any significant impairment to the integrity or availability of data, software, a system, or information." *Id.*

218. Under California's Consumer Protection Against Computer Spyware Act, a person or entity that is not an authorized user shall not, with actual knowledge, conscious avoidance of actual knowledge, or willfulness, collect personally identifiable information; prevent the blocking or disabling of software; take control of a consumer's computer; modify the settings of a computer related to its access or use of the internet; prevent a user from making reasonable efforts to block or disable software; or induce the installation of software. *See* Cal. Bus. & Prof. Code § 22947.3.

219. With actual knowledge, conscious avoidance of actual knowledge, and willfulness, Superfish and Lenovo caused VisualDiscovery to be copied onto Plaintiffs' and Class members' computers.

220. Lenovo and Superfish have committed the following violations of the Consumer Protection Against Computer Spyware Act through the creation and installation of VisualDiscovery:

221. Superfish collected, through intentionally deceptive means, personally identifiable information that includes all or substantially all of the Web sites visited by Plaintiffs and Class members, with VisualDiscovery installed in a manner designed to conceal its installation, in violation of Cal. Bus. & Prof. Code § 22947.2(b)(3).

222. Lenovo and Superfish prevented, without authorization and through intentionally deceptive means, Plaintiffs' and Class members' reasonable efforts to block the installation of and to disable VisualDiscovery by creating an opt-out process that was technically deficient and by causing the software to automatically reinstall or reactivate and remain on the computer after uninstallation, in violation of Cal. Bus. & Prof. Code § 22947.2(c).

223. Lenovo and Superfish intentionally misrepresented that VisualDiscovery would be uninstalled and disabled by Plaintiffs' and Class members' action of opting out, with the knowledge that the software would not be so uninstalled or disabled and would remain on their computers, in violation of Cal. Bus. & Prof. Code § 22947.2(d).

224. Superfish accessed Plaintiffs' and Class members' internet for the purpose of causing damage to their computers constituting the impairment of the integrity of their data and information, in violation of Cal. Bus. & Prof. Code § 22947.3(a)(2);

225. Lenovo and Superfish prevented Plaintiffs and Class members' reasonable efforts to block the installation of or disable Superfish by presenting them with the option to opt out of VisualDiscovery with knowledge that when that option was selected or users clicked outside of the opt-out window, the installation would nonetheless sometimes proceed, and falsely represented that the software had been disabled to Plaintiffs and Class members, in violation of Cal. Bus. & Prof. Code § 22947.3(c)(1)-(2).

226. Lenovo and Superfish induced Plaintiffs and Class members to install VisualDiscovery on computers by intentionally misrepresenting that the software was necessary to open, view, or play shopping content, in violation of Cal. Bus. & Prof. Code § 22947.4(a)(1).

227. As the actual and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered damages in an amount to be determined at trial.

COUNT VIII

VIOLATIONS OF CALIFORNIA'S INVASION OF PRIVACY ACT

Cal. Penal Code § 630, *et seq*.

(on behalf of Plaintiffs, the Indirect Purchaser Class, and the California Class Against Defendants Superfish and Lenovo)

228. Plaintiffs, the Indirect Purchaser Class, and the California Class incorporate by reference all allegations of the preceding and succeeding paragraphs as though fully set forth herein.

229. Plaintiffs bring this claim on behalf of themselves, the Indirect Purchaser Class, and the California Class against Superfish and Lenovo.

230. Plaintiffs and Class members sent web communications or received them within California.

231. Under California's Invasion of Privacy Act ("CIPA"), it is unlawful to intentionally, willfully, and without consent tap or make any unauthorized connection by means of any machine, instrument, or contrivance, or in any other manner with any telegraph or telephone wire, line, cable, or instrument, in order to purposefully intercept a communication or its content that is in transit or passing over any wire, line, or cable, or is being sent from or received within California; and to use, attempt to use, or communicate any such information obtained by these means. *See* Cal. Penal Code § 631.

232. Superfish violated CIPA intentionally, willfully, and without consent through the installation and operation of VisualDiscovery, which made unauthorized connections with Plaintiffs' and Class members' internet connections to purposefully intercept communications and their contents while they were in transit on web browsers. *See* Cal. Penal Code § 631. Furthermore, Superfish used, attempted to use, and communicated the information it obtained through VisualDiscovery to create pop-up shopping windows in Plaintiffs' and Class members' web browsers.

233. Lenovo aided, agreed with, or conspired with Superfish to unlawfully do, or permit, or cause to be done any and all of the acts discussed herein which violate CIPA. Cal. Penal Code. § 631(a)

("Any person who . . . aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, . . .").

234. As an actual and proximate result of the above actions, Plaintiffs and Class members have been injured and suffered actual damages in an amount to be determined at trial. For each violation of CIPA by Superfish and Lenovo, Plaintiffs and Class members are entitled to damages pursuant California Penal Code § 637.2 of $5,000 or three times the amount of their actual damages (at their election). *See* Cal. Penal Code § 637.2. Plaintiffs and Class members are also entitled to injunctive relief. *Id.*

COUNT IX

NEGLIGENCE UNDER CALIFORNIA LAW

(on behalf of Plaintiffs, the Indirect Purchaser Class, and the California Class Against Defendants Lenovo and Superfish)

235. Plaintiffs, the Indirect Purchaser Class, and the California Class incorporate by reference all allegations of the preceding and succeeding paragraphs as though fully set forth herein.

236. Plaintiffs bring this claim on behalf of themselves, the Indirect Purchaser Class, and the California Class against Lenovo and Superfish.

237. Lenovo owed a duty to all foreseeable users of Lenovo computers to take reasonable measures in accordance with industry standards ensure that the software installed on Lenovo computers did not interfere with the privacy and security of users' data and did not impede the performance and battery life of computers.

238. Superfish owed a duty to all foreseeable users of VisualDiscovery to take reasonable measures in accordance with industry standards to ensure that the software did not access private and secure information transmitted over websites, and to ensure that the software did not expose users to the risk of hacking by third parties through creating vulnerabilities in the transmission of their information.

239. Plaintiffs and Class members were foreseeable users of Lenovo computers and VisualDiscovery and fall within the class of persons to whom Lenovo and Superfish owed a duty of due care as described above.

240. Lenovo breached the duty it owed to Plaintiffs and Class members by failing to exercise reasonable care in overseeing Superfish in the installation and operation of the VisualDiscovery software, exposing Plaintiffs and Class members to privacy violations and security risks and impairing the functionality of their computers.

241. Superfish breached the duty it owed to Plaintiffs and Class members by accessing their private information transmitted over secure websites for the purposes of creating pop-up advertisements, and using inadequate security procedures that were not reasonable and did not conform to industry standards in accessing this information, thereby intruding on Plaintiffs' and Class members' privacy and risking the security of their information.

242. Lenovo's and Superfish's breach of duty was the actual, substantial, and proximate cause of injuries to Plaintiffs and Class members because these injuries stemmed from and were a foreseeable result of Defendants' breach.

243. As a result of Lenovo's and Superfish's breach, Plaintiffs and Class members have suffered direct and measurable loss and are entitled to damages, including compensation for the reduction in value of their computers during the time period that VisualDiscovery was installed and money expended to hire professionals to uninstall VisualDiscovery. Such damage does not constitute mere economic loss because the privacy and security violations exposed Plaintiffs and Class members to risk of the breach of their information by web hackers.

COUNT X

TRESPASS TO CHATTELS UNDER CALIFORNIA LAW

(on behalf of Plaintiffs, the Indirect Purchaser Class, and the California Class Against Defendants Lenovo and Superfish)

244. Plaintiffs, the Indirect Purchaser Class, and the California Class incorporate by reference all allegations of the preceding and succeeding paragraphs as though fully set forth herein.

245. Plaintiffs bring this claim on behalf of themselves, the Indirect Purchaser Class, and California Class against Lenovo and Superfish.

246. Plaintiffs and class members maintained actual or constructive possession of their Lenovo computers during the time period that VisualDiscovery was installed on them.

247. Lenovo and Superfish intentionally interfered with Plaintiffs' and Class members' use of their computers by installing and operating VisualDiscovery.

248. Plaintiffs and class members did not consent to this interference.

249. This interference was the actual and proximate cause of injury to Plaintiffs and Class members because it actually and substantially harmed the functioning of the computers by slowing down their internet speeds and reducing their battery life, impairing the computers' condition, quality, and value. This interference also actually and proximately injured Plaintiffs and Class because it exposed their private web data to privacy violations and security breaches, thus reducing the condition, quality, and value of the computers for the time period that VisualDiscovery was installed on them.

250. Plaintiffs and Class members are entitled to recover the actual damages they suffered as a result of Defendants' interference with their computers in an amount to be determined at trial.

COUNT XI

VIOLATION OF DECEPTIVE ACTS & PRACTICES STATUTE

N.Y. GEN. BUS. LAW § 349

(on behalf of Plaintiffs, the Direct Purchaser Class, and the New York Class Against Defendants Lenovo and Superfish)

251. Plaintiffs, the Direct Purchaser Class, and the New York Class incorporate by reference each preceding and succeeding paragraph as though fully set forth herein.

252. Plaintiffs bring this claim on behalf of themselves, the Direct Purchaser Class, and New York Class against Lenovo and Superfish.

253. Plaintiffs and Class members are "persons" within the meaning of N.Y. Gen. Bus. § 349(g).

254. Lenovo is a "person, firm, corporation, or association within the meaning of N.Y. Gen. Bus. § 349(b). Superfish is a "person, firm, corporation or association or agent or employee thereof" within the meaning of N.Y. Gen. Bus. § 349(b).

255. Under the New York Deceptive Acts & Practices Statute, "[d]eceptive acts and practices in the conduct of any business, trade or commerce or in the furnishing of any service" are unlawful. N.Y. Gen. Bus. § 349.

256. Defendants engaged in deceptive acts and practices in the conduct of business, trade, and commerce by secretly preinstalling VisualDiscovery on computers, violating Plaintiffs' and Class members' privacy without their knowledge or consent and exposing their data to security risks. Defendants also engaged in deceptive acts and practices by impairing the power use and internet speed of Plaintiffs' and Class members' computers through the installation of VisualDiscovery.

257. These acts and practices were consumer-oriented because they had a broad impact on consumers at large, affecting all users of Lenovo computers with VisualDiscovery preinstalled.

258. Defendants' acts and practices were misleading in a material respect because they were highly deceptive to a reasonable consumer acting reasonably under the circumstances, who could not anticipate that a new computer was preloaded with intrusive software that materially affected the performance of the computers and consumers' privacy and data security.

259. Defendants' deceptive acts and practices were willful and knowing because Defendants preinstalled VisualDiscovery and subsequently failed to uninstall the software from users' computers or correct its security and performance flaws despite their awareness of the massive functionality problems, privacy violations, and security risks of VisualDiscovery.

260. Plaintiffs and Class members were injured as a direct and proximate result of Defendants' deceptive acts and practices because, among other reasons, they received computers worth less than they bargained for and have spent money to remove VisualDiscovery and obtain antivirus software.

261. Plaintiffs and Class members are entitled to injunctive relief and to actual damages or fifty dollars per violation (at their election) because of Defendants' deceptive acts and practices. *See* N.Y. Gen. Bus. § 349(h). Plaintiffs and Class members are also entitled to treble damages because Defendants' actions were willful and knowing. *See id.* Finally, Plaintiffs and the other Class members are entitled to reasonable costs and attorney's fees. *See id.*

COUNT XII

NEGLIGENCE UNDER NEW YORK LAW

(on behalf of Plaintiffs, the Direct Purchaser Class, and the New York Class Against Defendants Lenovo and Superfish)

262. Plaintiffs, the Direct Purchaser Class, and the New York Class incorporate by reference all allegations of the preceding and succeeding paragraphs as though fully set forth herein.

263. Plaintiffs bring this claim on behalf of themselves, the Direct Purchaser Class, and New York Class members against Lenovo and Superfish.

264. Lenovo owed a duty to all foreseeable users of Lenovo computers to take reasonable measures in accordance with industry standards ensure that the software installed on Lenovo computers did not interfere with the privacy and security of users' data and did not impede the performance and battery life of computers.

265. Superfish owed a duty to all foreseeable users of VisualDiscovery to take reasonable measures in accordance with industry standards to ensure that the software did not access private and secure information transmitted over websites, and to ensure that the software did not expose users to the risk of hacking by third parties through creating vulnerabilities in the transmission of their information.

266. Plaintiffs and Class members were foreseeable users of Lenovo computers and VisualDiscovery and fall within the class of persons to whom Lenovo and Superfish owed a duty of due care as described above.

267. Lenovo breached the duty it owed to Plaintiffs and Class members by failing to exercise reasonable care in overseeing Superfish in the installation and operation of the VisualDiscovery software, exposing Plaintiffs and Class members to privacy violations and security risks and impairing the functionality of their computers.

268. Superfish breached the duty it owed to Plaintiffs and Class members by accessing their private information transmitted over secure websites for the purposes of creating pop-up advertisements, and using inadequate security procedures that were not reasonable and did not conform to industry standards in accessing this information, thereby intruding on Plaintiffs' and Class members' privacy and risking the security of their information.

269. Lenovo's and Superfish's breach of duty was the actual and proximate cause of injuries to Plaintiffs and Class members because these injuries stemmed from and were a foreseeable result of Defendants' breach.

270. As a result of Lenovo's and Superfish's breach, Plaintiffs and Class members have suffered direct, measurable, and compensable loss and are entitled to damages, including compensation for a reduction in value of their computers during the time period that VisualDiscovery was installed and money expended to hire professionals to uninstall VisualDiscovery.

COUNT XIII

TRESPASS TO CHATTELS UNDER NEW YORK LAW

(on behalf of Plaintiffs, the Direct Purchaser Class, and the New York Class Against Defendants Lenovo and Superfish)

271. Plaintiffs, the Direct Purchaser Class, and the New York Class incorporate by reference all allegations of the preceding and succeeding paragraphs as though fully set forth herein.

272. Plaintiffs bring this claim on behalf of themselves, the Direct Purchaser Class, and New York Class against Lenovo and Superfish.

273. Plaintiffs and Class members maintained actual or constructive possession of their Lenovo computers during the time period that VisualDiscovery was installed on them.

274. Lenovo and Superfish intentionally interfered with Plaintiffs' and Class members' use of their computers by installing and operating VisualDiscovery.

275. Plaintiffs and Class members did not consent to this interference.

276. This interference was the actual and proximate cause of injury to Plaintiffs and Class members because it actually and substantially harmed the functioning of their computers by slowing down internet speeds and reducing battery life, impairing Plaintiffs' and Class members' materially valuable interest in the computers' condition, quality, and value. This interference also actually and proximately injured Plaintiffs and Class because the interference exposed private web data to privacy violations and security breaches and reduced Plaintiffs' and Class members' materially valuable interest in the condition, quality, and value of the computers for the time period that VisualDiscovery was installed on them.

277. Plaintiffs and Class members are entitled to recover the actual damages they suffered as a result of Defendants' interference with their computers in an amount to be determined at trial.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and all others similarly situated, respectfully request that this Court:

A. Certify this action as a class action and appoint Plaintiffs' Interim Co-lead counsel as Class counsel;

B. Enter judgment in favor of Plaintiffs and the Classes against Defendants;

C. Award to Plaintiffs and the members of the Classes actual, statutory, treble, and punitive damages; and

D. Grant pre- and post-judgment interest, reasonable attorneys' fees and costs, and such other and further relief as this case may require and the Court may deem just and proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a jury trial on all issues so triable.

Dated: November 12, 2015

Respectfully submitted,

PRITZKER LEVINE LLP

/s/ Jonathan K. Levine

Jonathan K. Levine (SBN 220289)
Elizabeth C. Pritzker (SBN 146267)
Shiho Yamamoto (SBN 264741)
180 Grand Avenue, Suite 1390
Oakland, California 94612
Telephone: (415) 692-0772
Facsimile: (415) 366-6110
jkl@pritkzkerlevine.com
ecp@pritzkerlevine.com
sy@pritzkerlevine.com

GIRARD GIBBS LLP

/s/ Daniel C. Girard

Daniel C. Girard (SBN 114826)
Amanda M. Steiner (SBN 190047)

Elizabeth A. Kramer (SBN 293029)
Andre M. Mura (SBN 298541)
601 California Street, Suite 1400
San Francisco, CA 94104
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
dcg@girardgibbs.com
as@girardgibbs.com
eak@girardgibbs.com
amm@classlawgroup.com

COTCHETT, PITRE & McCARTHY, LLP

/s/ Matthew K. Edling

Steven N. Williams (SBN 175489)
Matthew K. Edling (SBN 250940)
Alexandra P. Summer (SBN 266485)
San Francisco Airport Office Center
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Telephone: (650) 697-6000
Facsimile: (650) 697-0577
swilliams@cpmlegal.com
medling@cpmlegal.com
asummer@cpmlegal.com

Plaintiffs' Interim Co-lead Counsel